IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MICHAEL WIGGINS and TERI STEVENS, individually and for all others similarly situated, **Plaintiffs,** **v.** **LABORATORY CORPORATION OF AMERICA HOLDINGS,** **Defendant.**	**Case No. _____**

CLASS ACTION COMPLAINT

Michael Wiggins and Teri Stevens ("Plaintiffs"), by and through their undersigned counsel, hereby bring this action against Laboratory Corporation of America Holdings ("Labcorp" or "Defendant"), alleging as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this action for themselves, and for thousands of other patients whose medical privacy Labcorp has violated for the sake of profit.

2. In a nutshell, Labcorp installed three types of Google computer code, called Google Analytics, Google Ads, and Google Display Ads ("Google Collection Tools"), on its public website, *https://www.labcorp.com/*. This computer code, designed by Google with input from Labcorp, intercepts an array of individually-identifiable health information from all Labcorp website users and sends this information to Google.[1] Google then uses "cookies" to match this

[1] Google Collection Tools collect an extensive array of information from each visitor to Labcorp's website, device identifiers, advertising ID, Google account IDs, e-mail address, phone number, demographic information, searches performed, links clicked, web pages viewed, information typed into text boxes, appointments made, medical tests and treatments, test results, medical conditions, health insurance, and payment information. This information is collected and sent from Labcorp's website to Google instantaneously, and without notice or consent.

information to individual users, build-out the profiles of Google account holders, analyze the individually-identifiable health information from Labcorp's website, and share this analysis with Labcorp so both companies can put these patients' individually-identifiable health information to multiple uses, commercial and otherwise, that include: determining how patients use Labcorp's website, determining which advertisements they see, and selling targeted advertisements to companies interested in showcasing their products to individuals sharing certain characteristics.[2]

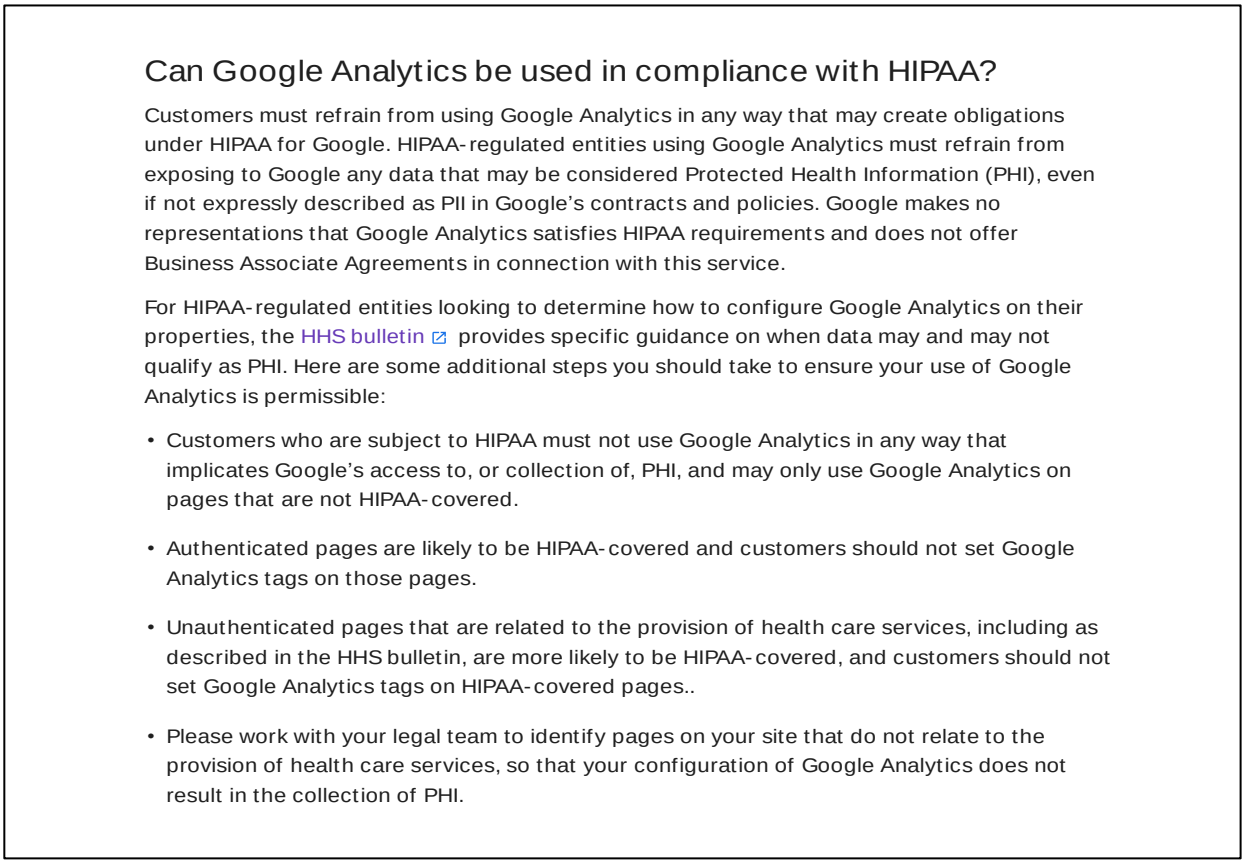
3. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996) and Pennsylvania law requiring the confidential treatment of medical records, 28 Pa. Code § 115.27, both expressly prohibit healthcare providers from sharing individually-identifiable health information with third parties except as needed for a patient's treatment, payment, or with their authorization. Importantly, the protections these laws provide give patients a reasonable expectation of privacy in communications with healthcare providers relating to their medical conditions and treatment.

4. The United States Department of Health and Human Services ("HHS") recently confirmed that HIPAA and its regulations have long prohibited the transmission of individually-identifiable health information by tracking technology, like performed by the Google Collection Tools, without a patient's express authorization.[3]

[2] For example, a person diagnosed with diabetes will be sent advertisements for diabetic care products, treatments, or services. These "targeted" advertisements are sold for a premium as compared to non-targeted advertisements because, by virtue of their diagnosis, the recipients are more likely to need, and therefore purchase, the advertised product.

[3] *See* Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.*

5. In recognition of these long-existing prohibitions and protections, Google has expressly warned all HIPAA-covered entities, including Labcorp, that using Google Collection Tools can violate HIPAA:



Can Google Analytics be used in compliance with HIPAA?

Customers must refrain from using Google Analytics in any way that may create obligations under HIPAA for Google. HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI), even if not expressly described as PII in Google's contracts and policies. Google makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business Associate Agreements in connection with this service.

For HIPAA-regulated entities looking to determine how to configure Google Analytics on their properties, the HHS bulletin provides specific guidance on when data may and may not qualify as PHI. Here are some additional steps you should take to ensure your use of Google Analytics is permissible:

- Customers who are subject to HIPAA must not use Google Analytics in any way that implicates Google's access to, or collection of, PHI, and may only use Google Analytics on pages that are not HIPAA-covered.
- Authenticated pages are likely to be HIPAA-covered and customers should not set Google Analytics tags on those pages.
- Unauthenticated pages that are related to the provision of health care services, including as described in the HHS bulletin, are more likely to be HIPAA-covered, and customers should not set Google Analytics tags on HIPAA-covered pages..
- Please work with your legal team to identify pages on your site that do not relate to the provision of health care services, so that your configuration of Google Analytics does not result in the collection of PHI.

FIG. 1.[4]

6. During the period at issue in this lawsuit, Google's Terms of Service, Data Policy, and Cookies Policy did not inform its users or account holders that it could acquire their health information without notice or consent when they interacted with a healthcare provider's website or application.

[4] HIPAA and Google Analytics, available at *https://support.google.com/analytics/answer/13297105?hl=en* (last accessed February 5, 2024).

7. During the period at issue in this lawsuit, Labcorp's Terms and Conditions, Notice of Privacy Practices, and Web Privacy Statement did not inform its website users that it was using their individually-identifiable health information for commercial purposes, sharing their individually-identifiable health information with Google, or allowing Google to use this information for commercial purposes. Instead, Labcorp's public-facing policy statements repeatedly promised that its website was a safe, secure place to communicate health information, that it treated patients' individually-identifiable health information as private and confidential, and that it would not share this information, or allow it to be used for commercial purposes, without notice and consent.[5]

8. Labcorp's interception, dissemination, and commercial use of its patients' individually-identifiable health information without notice or consent violates federal and state law, harms patients by intruding upon their privacy, erodes the confidential nature of the provider-patient relationship, violates patients' property rights, deprives patients of their right to control dissemination of their individually-identifiable health information, and requires decisive corrective action by this Court.

JURISDICTION AND VENUE

9. 28 U.S.C. § 1331 provides this Court with subject matter jurisdiction over claims based on the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*.

10. 28 U.S.C. § 1332(d) provides this Court with subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(d), 1453 and 1711-15 ("CAFA") because

[5] *See* Labcorp's Notice of Privacy Practices, *https://www.lab corp.com/about/hipaa-information* (Jan. 31, 2020) (Labcorp "is required by law to maintain the privacy of health information that identifies you," "is committed to the protection of your [protected health information] and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation").

the proposed class includes at least 100 members, at least one class member is a citizen of a different state than defendant, and the amount in controversy exceeds $5,000,000.00, exclusive of interest and costs.

11. Venue is proper in this District under 28 U.S.C. § 1391, because Defendant does business in this District, subjecting it to personal jurisdiction. Venue is also proper in this District, because a substantial part of the events or omissions giving rise to the claim occurred in, and emanated from, this District.

THE PARTIES

12. Labcorp is a corporation headquartered in Burlington, North Carolina. Labcorp operates approximately 2,135 locations in 47 U.S. states that, in concert with one of the largest clinical laboratory networks in the world, perform millions of tests (and related services) each week, that include: general and specialty laboratory tests, bone marrow and human leukocyte antigen tests, clinical trial services, drug testing services, deoxyribonucleic acid identification services, forensic identity services, insurance health plan services, paternity testing services, patient services, personalized medicine, and hospital services. To facilitate these tests, Labcorp operates a website, *https://www.labcorp.com/*, where its established patients and the general public can find a lab, schedule test appointments, pay their bills, contact the Labcorp Customer Service team for help, or shop for more than 50 tests, covering everything from "Albumin/Creatinine Ratio" to "Vitamin Deficiency."

13. Michael Wiggins is a citizen of the Commonwealth of Pennsylvania. Mr. Wiggins has been a Labcorp patient and a *www.labcorp.com* user since at least 2016. During the relevant period, Mr. Wiggins used Labcorp's website to schedule appointments, request information on specific medical services, view test results, access his doctor's notes, and make payments for

medical services. By doing so, Mr. Wiggins' individually-identifiable health information was disclosed to Google under the systematic process described herein. Mr. Wiggins had no knowledge his sensitive medical information was shared with Google, or any other third parties, and did not authorize Labcorp to disclose his individually-identifiable health information to Google, or use this information for commercial purposes.

14. Teri Stevens is a citizen of the State of Maryland. Ms. Stevens has been a Labcorp patient and a *www.labcorp.com* user since at least 2011. During the relevant period, Ms. Stevens used Labcorp's website to schedule appointments, review test results, access her doctor's notes, and make payments for medical services. By doing so, Ms. Stevens' individually-identifiable health information was disclosed to Google under the systematic process described herein. Ms. Stevens had no knowledge her sensitive medical information was shared with Google, or any other third parties, and did not authorize Labcorp to disclose her individually-identifiable health information to Google, or use this information for commercial purposes.

BACKGROUND FACTS

Google Tracking And Analytics Tools Compile Extensive Personal Data To Enable Targeted Marketing Efforts

15. Google is one of the world's most prominent and recognizable brands, offering a plethora of internet services and products ranging from e-mail to software for mobile phones to cloud services for businesses.[6] From its inception, Google has been preoccupied with the idea of "extracting meaning from the mass of data accumulating on the Internet," and has made a lucrative industry out of this venture.[7]

[6] *See https://www.britannica.com/topic/Google-Inc* (accessed Jan. 12, 2024); *https://cloud.google.com/?utm_source=about&utm_medium=referral&utm_campaign=footer-link*.

[7] *See https://www.britannica.com/topic/Google-Inc* (accessed Jan. 12, 2024).

16. Google has expanded its search engine business into advertising by combining various marketing and advertisement firms' databases of information to tailor ads to consumers' individual needs and preferences.[8] Google has spent billions of dollars to acquire these web advertisement firms, services, and networks.[9] In 2000, Advertising on Google was launched with the aim of connecting online businesses with users through "highly targeted ad serving technology" that enabled advertisers to monitor ad statistics such as click-through rates and visitor interest.[10] Since around 2015, Google has been the market leader in online advertising, earning nearly all its revenue from selling targeted ads based on Google users' search requests.[11]

17. Google offers several platforms and analytics for advertisers to optimize their advertising campaigns.[12] Advertisers using Google products can bid on specific search words and phrases that lead their ads to be more prominently displayed to relevant users in search results.[13]

---

[8] *Id.*

[9] *Id.*

[10] *See https://www.blog.google/technology/ads/new-advertising-brands/* (accessed Jan. 18, 2024); *http://googlepress.blogspot.com/2000/10/google-launches-self-service.html* (accessed Jan. 18, 2024).

[11] *See* How Google's $150 Billion Advertising Business Works, *https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-break down-html* (accessed Jan. 18, 2024); *https://www.britannica.com/topic/Google-Inc* (accessed Jan. 18, 2023).

[12] *See https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html* (accessed Jan. 18, 2024).

[13] *Id.*

18. Google's search advertising capabilities are so powerful they enable advertisers to target a specific location, language, and/or audience.[14] Google's ads are not just embedded within Google search results, but also within other Google features such as Google Maps and YouTube.[15]

19. Google prides itself on its "advanced" analytics products and services to provide advertisers a "holistic view into consumer behavior" to better target them.[16] To optimize advertising, Google offers data tracking features that track how users interact with ads and advertisers' websites. For instance, Google will track and analyze what words or ads drove the most sales for any given Google customer and what days users clicked on search ads the most. Google can track groups of users "who have generated similar behavioral data or who share demographic or other descriptive data," *e.g.*, age group and gender.[17] In essence, Google's mining of user data is what drives and makes Google's targeted advertising so precise.

20. Google's data collection capabilities also include tracking user actions on customer websites and apps that are referred to as "events," and important desired events (such as purchases)

---

[14] *Id.*

[15] *See https://www.business.com/articles/6-reasons-why-your-business-should-be-using-google-adwords/* (accessed Jan. 18, 2024).

[16] *See https://blog.google/products/ads-commerce/5-tips-to-power-your-2023-marketing-strategy/?ga=2.25524031.381 675576.1689225706-1533121624.1689225706* (accessed Jan. 18, 2024).

[17] *See https://support.google.com/analytics/answer/12799087?hl=en&sjid=354832994521024 1384-NA* (accessed Jan. 19, 2023).

that are referred to as "conversions."[18] Tracked conversions can be used to measure the effectiveness of ads and monitor user behavior.[19]

21. Google generates reports to give its advertising customers "post-click performance metrics for users who clicked on [a]ds and then came through [an advertiser's] website, or installed and started using [an advertiser's] mobile app."[20] Google's data collecting and reporting capabilities are encapsulated in its Google Analytics service.

22. Google Analytics is a suite of business tools, a "platform that collects data from [advertisers'] websites and apps to create reports that provide insights into [their] business, that Google claims will help website owners understand how visitors use their sites and apps.[21] For example, Google Analytics helps website owners "understand which sections of an online newspaper have the most readers, or how often shopping cards are abandoned for an online store."[22]

---

[18] *See https://support.google.com/analytics/answer/13128484?sjid=11475162976737609263-NA* (accessed August 17, 2023).

[19] *See https://support.google.com/analytics/answer/13128484?sjid=11475162976737609263-NA* (accessed Jan. 19, 2023); *ttps://support.google.com/analytics/answer/13366706?sjid=11475162976737609263-NA* (accessed Jan. 19, 2023).

[20] *See https://support.google.com/analytics/answer/4355493?hl=en&ref_topic=1308583&sjid=11475162976737609263-NA* (accessed Jan. 19, 2023).

[21] *See* Some Facts About Google Analytics Data Privacy, *https://blog.google/around-the-globe/google-europe/google-analytics-facts/* (accessed Jan. 19, 2024); https://support.google.com/analytics/answer/12159447?hl=en (accessed Jan. 19, 2024).

[22] *Id.*

23. Google Analytics allows its customers to collect detailed information like the number of clicks, scrolls, searches, and downloads a site user performs.[23] The most recent version of Google Analytics offers a feature called "Reporting Identity," that helps customers identify users by "creat[ing] a single user journey from all the data associated with the same identity."[24]

24. Google Analytics offers advertisers machine learning technology to uncover and predict new user insights such as their behavior and identifies new audiences of users likely to make a purchase.[25]

25. Another tool Google offers is the Google Analytics embedded pixel, an invisible 1x1 web "bug" that website owners can add to the code on each page of their website to measure certain actions users take on the site, like online purchases.[26] The tracking pixel is a default feature of Google Analytics.[27]

26. Google explains the Google Analytics embedded pixel as follows: "Every time a user visits a webpage [with the code], the tracking code *will collect* [purportedly] *pseudonymous information about how that user interacted with the page*.[28] The tracking pixel

---

[23] *See https://www.mparticle.com/blog/google-tag-manager-vs-google-analytics/#:~:text=Google%20Analytics%20is%20an%20analytics,for%20granular%20user%20event%20insights%20* (accessed Aug. 17 2023).

[24] *Id.*

[25] *See https://blog.google/products/ads-commerce/prepare-for-future-with-google-analytics-4/* (accessed August 17, 2023).

[26] *See https://support.google.com/analytics/answer/12159447?hl=en* (accessed Jan. 19, 2024).

[27] *Id.*

[28] *Id.*

will also collect information from the browser like the language setting, the browser type, and the device and operating system on which the browser is running.[29]

27. The Google Analytics embedded pixel can even collect the "traffic source," which is what brought users to the site in the first place, such as a search engine, an advertisement they clicked on, or an e-mail marketing campaign.[30] "When the tracking pixel collects data, it packages the information and sends it to Google Analytics to be processed into reports."[31] The reports are then organized on particular criteria like whether a user's device is mobile or desktop, or which browser they are using.[32] A Google Analytics customer can further configure the settings to allow them to customize what data is collected and how it is processed.[33]

28. The vast capabilities of the Google Analytics tracking pixel allow it to collect up to 200 different metrics of user data, including:

- Ad Interactions – Includes when users are exposed to ads, when users click ads, and when ads grant rewards.
- Button Click Data – Includes when users click links that lead outside of the current domain, when users click links leading to files, how often buttons are clicked, tracking common clicks, any buttons clicked by site visitors, when screen transitions occur, every time a user's page loads or is changed by the active site, when a user scrolls to the bottom of a page, each time a user performs a site search, first time site visits, and when users use and submit forms
- Enabling Options – Google Analytics allows customers to enable "enhanced measurements" which allow for the collection of other types of optional data. The optional enhanced measurements do not

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.*

> require code changes; instead, once the options are enabled Google Analytics begins collecting the data. Examples of Custom data events that can be collected include conversion events, page views based on browser history, scrolls, and site searches. [34]

29. The Google Analytics' pixel transmits user website interactions and data to Google in real time, so this information can be stored and processed into reports. Once the data is stored, it cannot be changed.[35]

30. Google Collection Tools are not simply "tools" website owners use for their own purposes. Google Collection Tools provides Google with data to power its algorithms, providing it insight into the habits of users across the internet. Indeed, the vast amounts of data Google obtains allows it to amass detailed dossiers, or "digital fingerprints," that it keeps on its users and website visitors. Google Source Code also includes a feature that allows it to integrate with other Google data, collecting products such as Google Ads, Google Data Studio, Google AdSense, Google Optimize 360, Google Ad Manager, and Google Search Console.[36]

Labcorp Installed Google Collection Tools On Its Website To Compile Extensive Personal Data From Its Patients

31. Labcorp has enabled an array of Google Collection Tools to collect extensive data from visitors to *https://www.labcorp.com/*.

---

[34] *See https://support.google.com/firebase/answer/9234069?sjid=13198096824834568666-NA&visit_id=638248819935482735-1615699485&rd=1* (accessed Jan. 19, 2023); *https://support.google.com/analytics/answer/9216061?sjid=13198096824834568666-NA* (accessed Aug. 17, 2023).

[35] *See https://support.google.com/analytics/answer/12159447?hl=en* (accessed Jan. 19, 2024).

[36] *See https://www.techtarget.com/searchbusinessanalytics/definition/Google-Analytics#:~:text=Google%20Analytics%20includes%20features%20that,and%20integration%20with%20other%20applications* (accessed Jan. 19, 2023).

32. The "cid" cookie, short for "Client ID," is a cookie Google assigns to a specific user. As Google admits in its Google Analytics documentation for web-developers, the "cid" cookie represents personal information:

> In order for Google Analytics to determine that two distinct hits belong to the same user, a unique identifier, associated with that particular user, must be sent with each hit. The analytics.js library accomplishes this via the Client ID field, a unique, randomly generated string that gets stored in the browser's cookies, *so subsequent visits to the same site can be associated with the same user.*[37]

33. The "_gid" cookie, short for "Google Analytics ID," is a unique identifier assigned to a user on a single website when the user is logged in to a Google service in the same browser they use to access the website. When this condition is met, the "_gid" cookie is assigned to the user, stored in a first-party cookie, and collected in all Google Analytics hits. If the user has "Ads Personalization" enabled in their Google account, this ID is used to associate pages viewed and actions taken with the user to enhance targeting and personalization by Google. When a website has "Google Signals" enabled in its Google Analytics property, this ID and associated data are used to enhance the audience creation and demographics reporting available to the website owner in Goggle Analytics.[38]

34. The specific individually-identifiable health information that Labcorp collects and sends to Google through the Google Collection Tools includes, but is not limited to:

a. log-ins to the Labcorp website;

b. appointments scheduled on the Labcorp website;

---

[37] *See https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id.*

[38] *See https://infotrust.com/articles/gdpr-and-google-analytics-is-it-really-illegal/#:~:text=Google%20Analytics%20ID%20(_gid)%20–%20this%20is%20a%20unique%20identifier,they%20are%20accessing%20the%20website.*

c. searches made for a test location on the Labcorp website;

d. test location selections on the Labcorp website;

e. test appointments made on the Labcorp website;

f. information entered in text boxes on the Labcorp website;

g. pages visited on the Labcorp website; and

h. buttons, links, and tabs selected or clicked on the Labcorp website.

Labcorp Violated Its Privacy Policies By Failing To Disclose The Full Scope Of Its Data Collection Efforts, Using Patients' Data For Undisclosed Purposes, Sharing Patient Data With Undisclosed Recipients, And Allowing Those Entities To Use Its Patients' Data For Their Own Undisclosed Purposes

35. To attract patients, enable their pursuit of medical care, foster its provision of that medical care, and support its business, Labcorp's website enables individual patients to engage in a wide array of communications concerning their individually-identifiable health information.

36. The Labcorp Terms and Conditions provides: "Our Privacy Statement and, with respect to protected health information, our Notice of Privacy Practices describe how Labcorp collects information about you through the Online Services, and how we use, disclose, and protect that information." *See* Labcorp Terms and Conditions, *https://www.labcorp.com/terms-and-conditions* (Sept. 30, 2021).

37. Labcorp's Notice of Privacy Practices explains: "Labcorp is required by law to maintain the privacy of health information that identifies you, called protected health information (PHI)… Labcorp is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation. We take this commitment seriously..." *See* Labcorp's Notice of Privacy Practices, *https://www.labcorp.com/about/hipaa-information* (Jan. 31, 2020).

38. Labcorp's Notice of Privacy Practices promises: "For… uses and disclosures of PHI for marketing purposes and disclosures that would constitute a sale of PHI, Labcorp will ask for patient authorization before using or disclosing PHI." *Id.*

39. Labcorp's Web Privacy Statement says: "We do not ask You to provide personal health care information to Us through our general website. We obtain personally identifying information about You only if You voluntarily choose to provide such information via correspondence with Us." *See* Labcorp Web Privacy Statement, *https://www.labcorp.com/about /web-privacy-policy* (Nov. 27, 2023).

40. Labcorp's Web Privacy Statement further explains that it will seek "explicit consent" before collecting "sensitive personal information (such as your… health information)." *Id.*

41. Labcorp's Web Privacy Statement omits to mention, explicitly or otherwise, of the Google pixel, the Google Collection Tools, or the fact that user website interactions or data are transmitted to Google or used for its commercial purposes, advising only that: "Labcorp [] uses [] Google Analytics [] to analyze traffic to the various Labcorp webpages. Data collected regarding site usage is compiled in aggregate to improve the performance of the site, create a profile of uses, and improve our marketing and advertisements."

42. Notwithstanding all these representations, Labcorp worked with Google to design and install Google Collection Tools on the Labcorp website that captured the "characteristics" of all visitors' communications (*i.e.*, their advertising ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.*, the information patients type into text boxes, and the URLs, buttons, links, pages, and tabs they click and view), and transmitted this individually-identifiable health information to Google.

43. For example, an existing patient who visited Labcorp's website to schedule an appointment would first click the "Patient Login" button at the top of Labcorp's home screen:

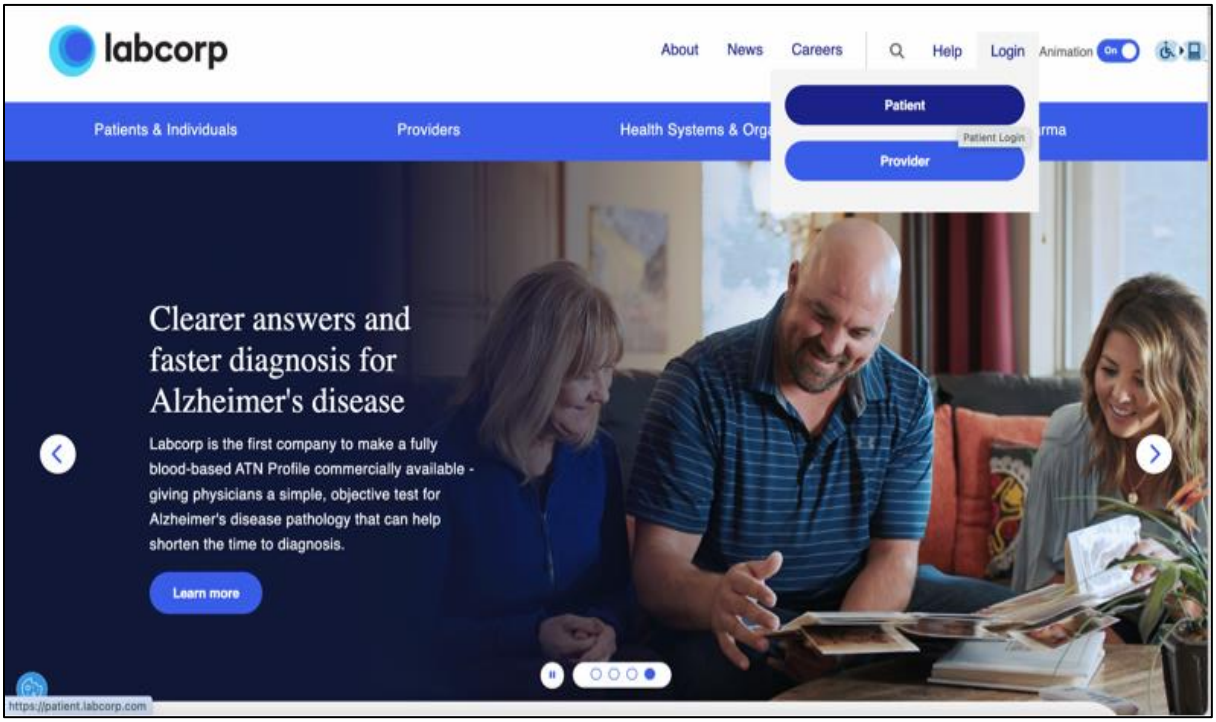


FIG. 2

44. Contemporaneously with the patient's click of the "Patient Login" button, Labcorp's Google Collection Tools intercept and transmit both the "contents" and "characteristics" of the login communication to Google including, among other things: the hit type ("t" or "event"), the document location URL ("dl" or "https://www.labcorp.com"), the document title ("dt" or "Lab Test Diagnostics, Biopharma & Global Life Sciences"), the event category ("ec" or "Patient Account"), the event action ("ea" or "Login Click"), the event label ("el" or "Patient"), and several identifiers that uniquely identify patients, such as the cid, tid, _gid, and gtm cookies. *See* Fig. 3.

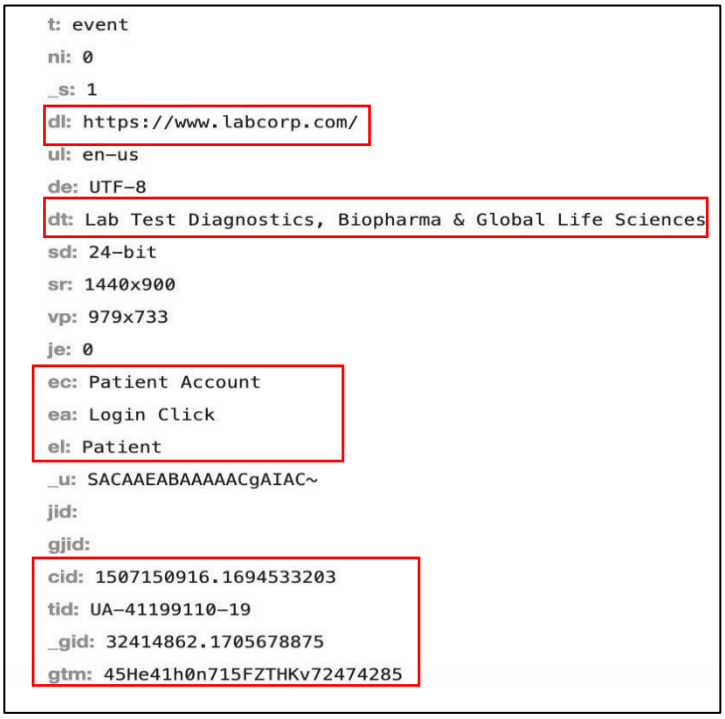


FIG. 3

45. To continue scheduling an appointment, the patient would then click the "Appointments" tab, click their name, and click the "Schedule Appointment" button. *See* Fig. 4.

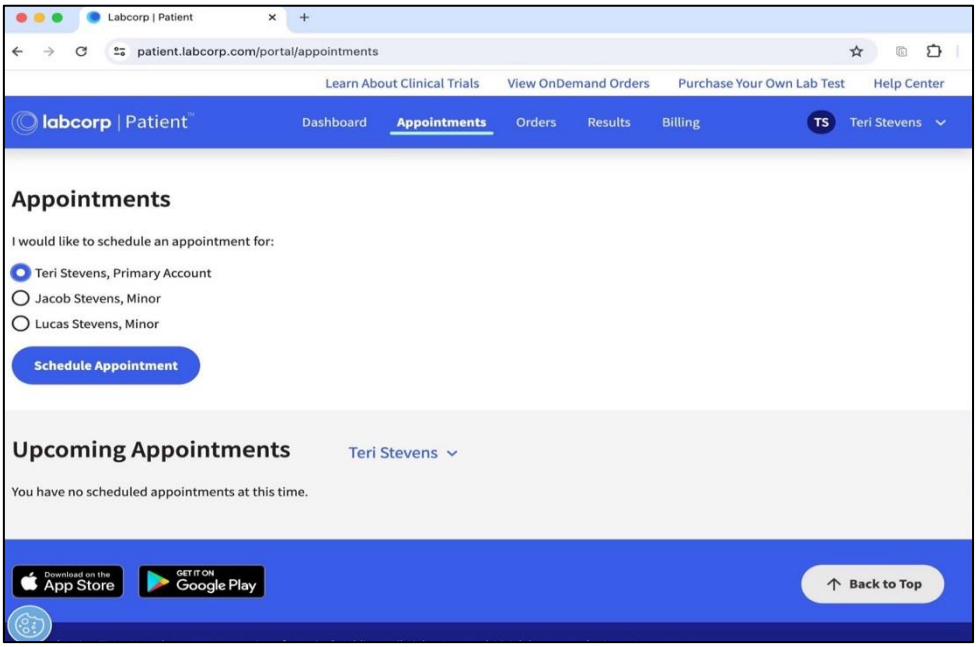


FIG. 4

46. Next, the website directs the patient to the "Find a Lab" page, where they are prompted to enter their zip code and the reason for their visit. *See* Fig. 5.

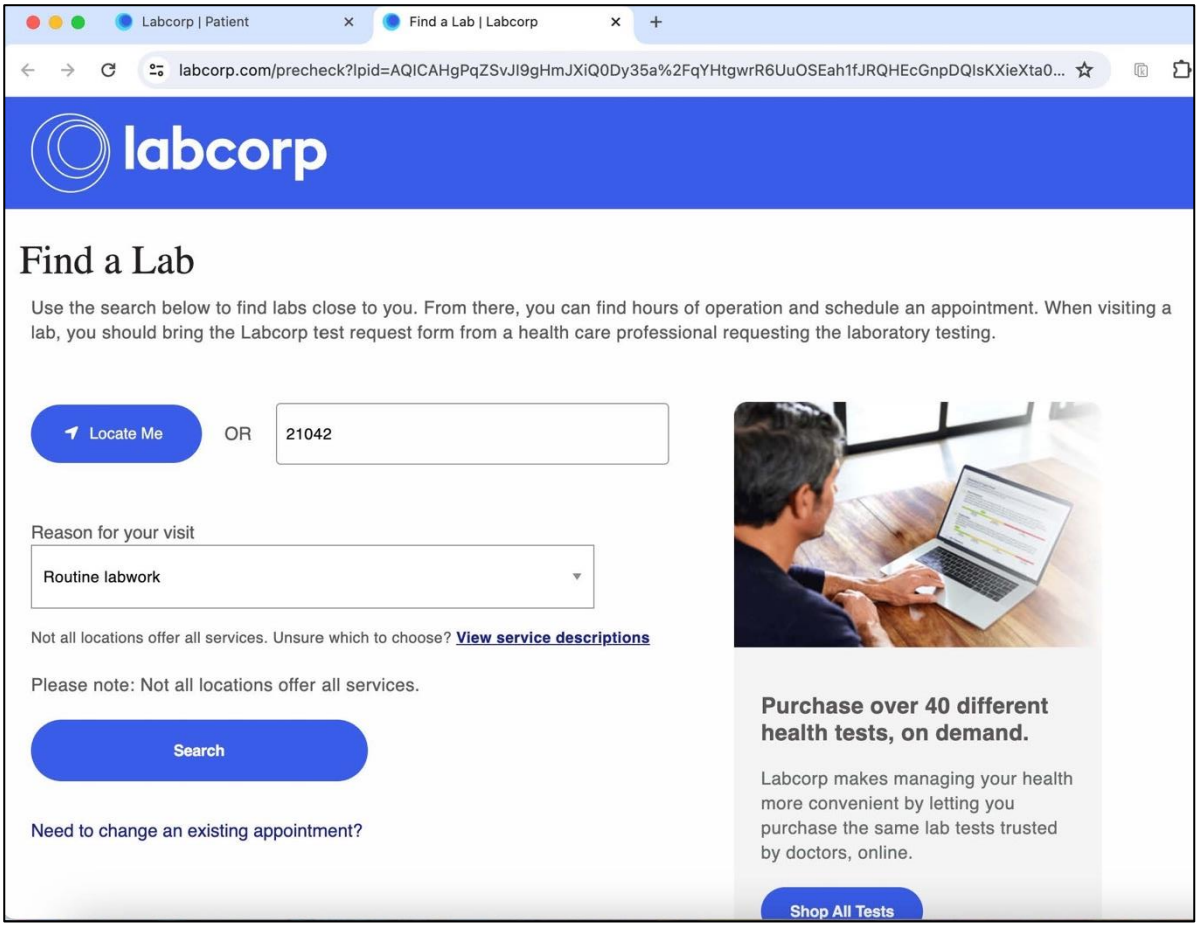


Fig. 5

47. Once the patient enters this information and hits the "Search" button, Labcorp's Google Collection Tools intercept and transmit both the "contents" and "characteristics" of the search communication to Google including, among other things: the descriptive URL the patient has asked to view, the patient's city, state, and zip code, and several identifiers that uniquely identify the patient, such as the cid, tid, _gid, jid, gjid, and gtm cookies. *See* Fig. 6.

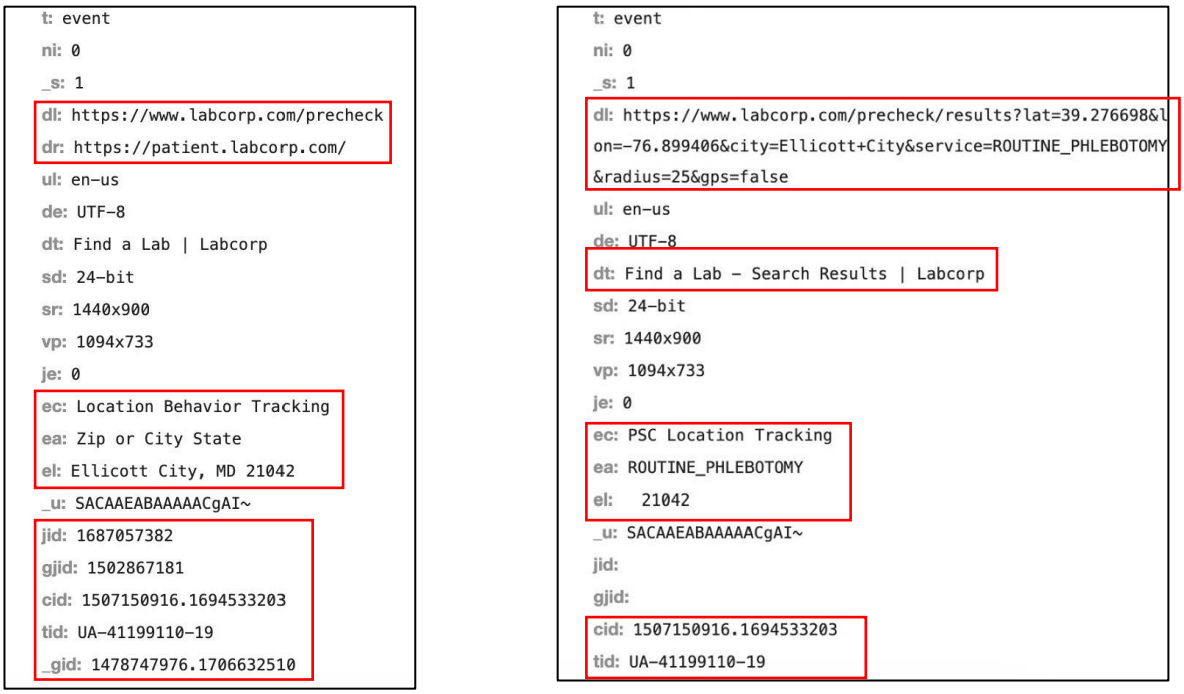


Fig. 6

48. From here, the patient is directed to a "Search Results" page that includes an interactive map featuring Labcorp locations near them offering the requested service(s). *See* Fig. 7.

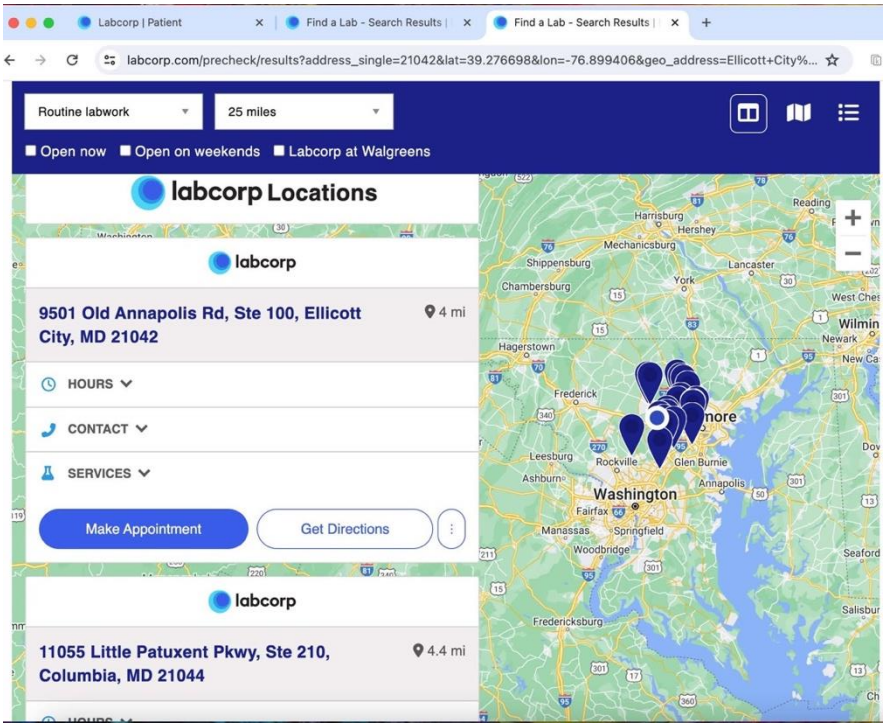


Fig. 7

49. Once the patient choses a location and clicks the "Make Appointment" button, Labcorp's Google Collection Tools intercept and transmit both the "contents" and "characteristics" of the search communication to Google including, among other things: the event action ("ea") informing Google the patient has clicked the "Make Appointment" button, the event label ("el") that shows a descriptive URL that describes the location for the appointment, the current location of the patient, the reason for their visit, and several identifiers that uniquely identify the patient, such as the cid, tid, _gid, jid, gjid, and gtm cookies. *See* Fig. 8.

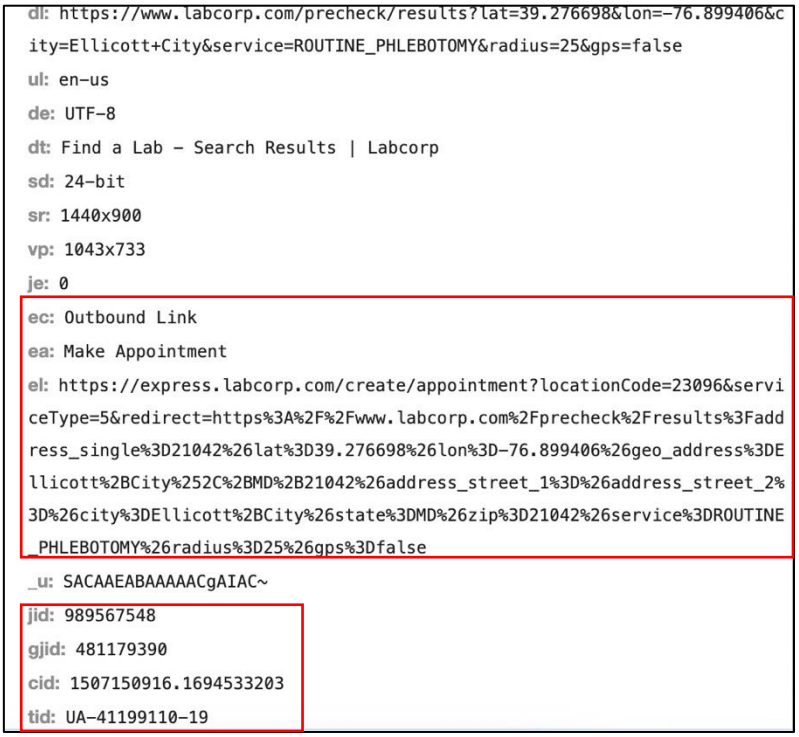


Fig. 8

50. The patient is then directed to the "Schedule an Appointment" page and asked to confirm the service requested, if they will be fasting, and the day and time for the appointment. *See* Fig. 9.

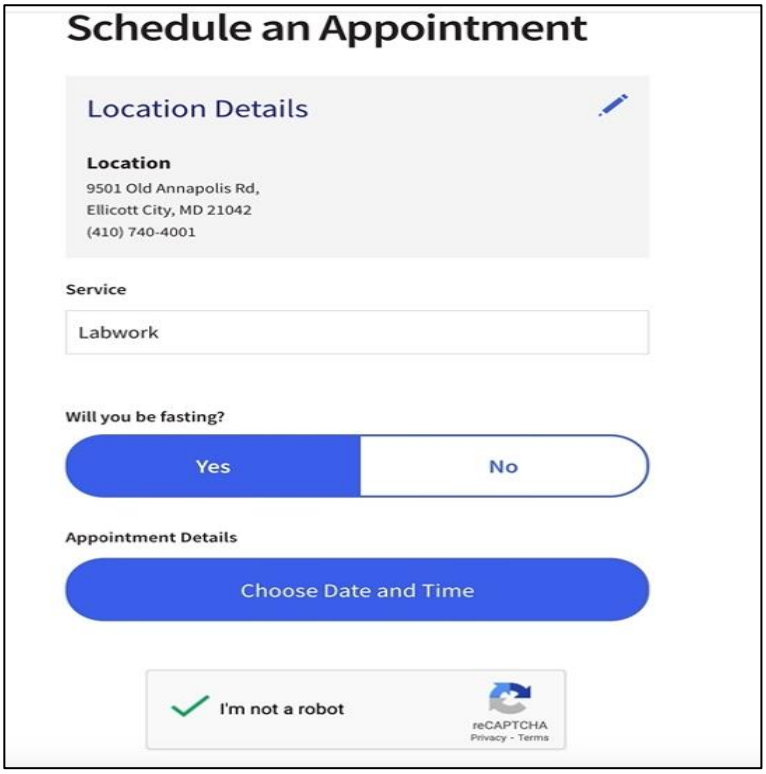
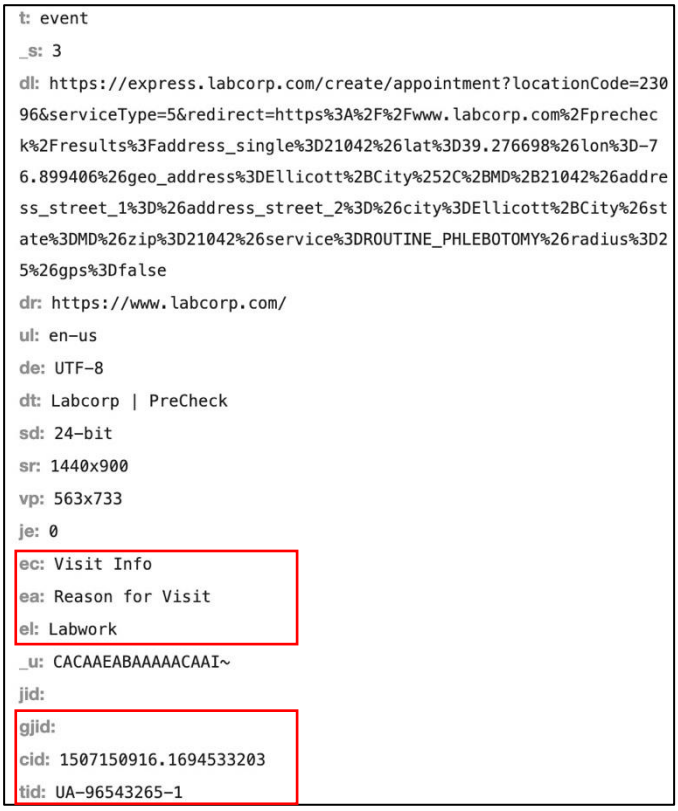
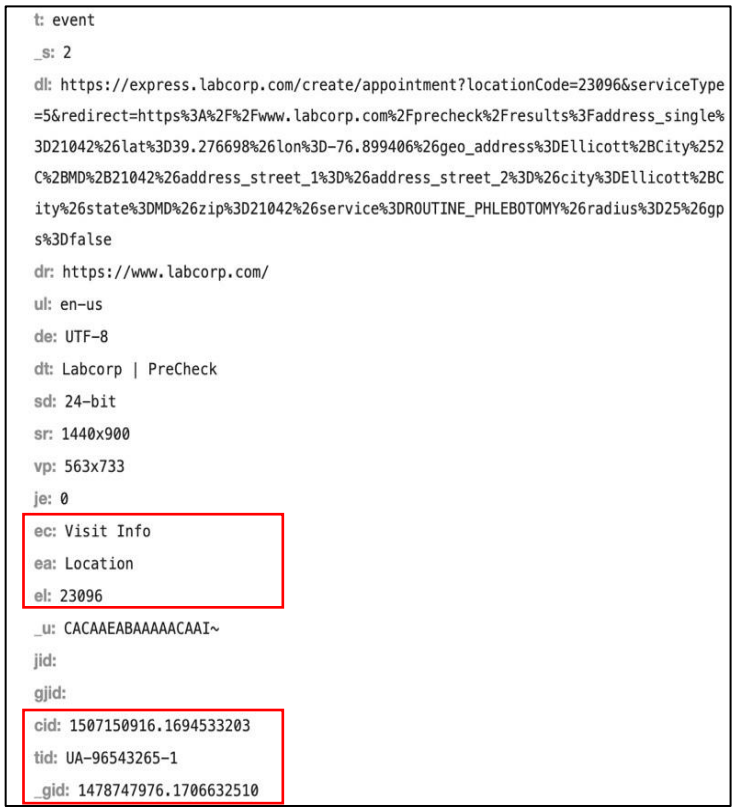


Fig. 9

51. Once the patient enters this information, Labcorp's Google Collection Tools intercept and transmit both the "contents" and "characteristics" of all the information the patient has entered into the form including, among other things: the patient's reason for making the appointment, a code identifying the location of the appointment, whether the patient will be fasting for the appointment, and several identifiers that uniquely identify the patient, such as the cid, tid, and _gid cookies. *See* Fig. 10.


t: event
_s: 3
dl: https://express.labcorp.com/create/appointment?locationCode=23096&serviceType=5&redirect=https%3A%2F%2Fwww.labcorp.com%2Fprecheck%2Fresults%3Faddress_single%3D21042%26lat%3D39.276698%26lon%3D-76.899406%26geo_address%3DEllicott%2BCity%252C%2BMD%2B21042%26address_street_1%3D%26address_street_2%3D%26city%3DEllicott%2BCity%26state%3DMD%26zip%3D21042%26service%3DROUTINE_PHLEBOTOMY%26radius%3D25%26gps%3Dfalse
dr: https://www.labcorp.com/
ul: en-us
de: UTF-8
dt: Labcorp | PreCheck
sd: 24-bit
sr: 1440x900
vp: 563x733
je: 0
ec: Visit Info
ea: Reason for Visit
el: Labwork
_u: CACAAEABAAAAACAAI~
jid:
gjid:
cid: 1507150916.1694533203
tid: UA-96543265-1


t: event
_s: 2
dl: https://express.labcorp.com/create/appointment?locationCode=23096&serviceType=5&redirect=https%3A%2F%2Fwww.labcorp.com%2Fprecheck%2Fresults%3Faddress_single%3D21042%26lat%3D39.276698%26lon%3D-76.899406%26geo_address%3DEllicott%2BCity%252C%2BMD%2B21042%26address_street_1%3D%26address_street_2%3D%26city%3DEllicott%2BCity%26state%3DMD%26zip%3D21042%26service%3DROUTINE_PHLEBOTOMY%26radius%3D25%26gps%3Dfalse
dr: https://www.labcorp.com/
ul: en-us
de: UTF-8
dt: Labcorp | PreCheck
sd: 24-bit
sr: 1440x900
vp: 563x733
je: 0
ec: Visit Info
ea: Location
el: 23096
_u: CACAAEABAAAAACAAI~
jid:
gjid:
cid: 1507150916.1694533203
tid: UA-96543265-1
_gid: 1478747976.1706632510

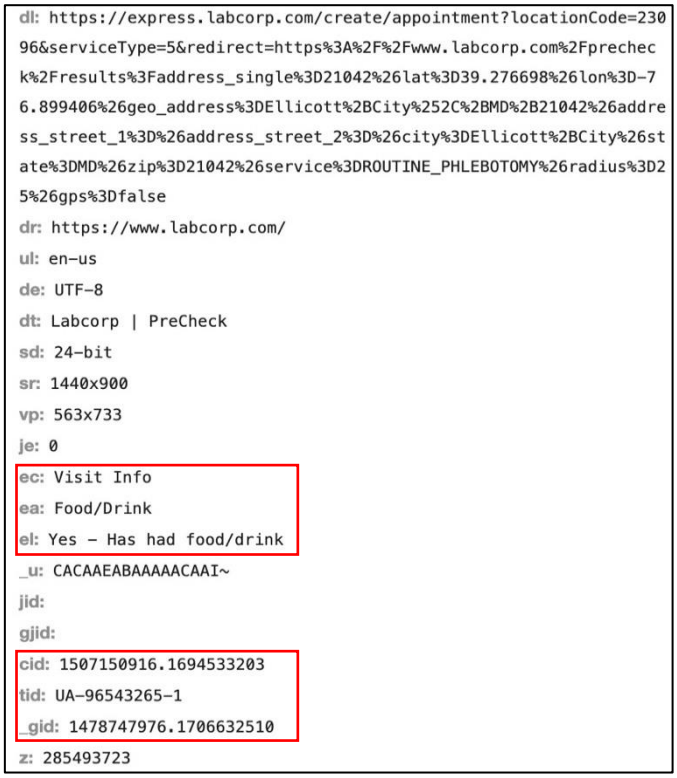

dl: https://express.labcorp.com/create/appointment?locationCode=23096&serviceType=5&redirect=https%3A%2F%2Fwww.labcorp.com%2Fprecheck%2Fresults%3Faddress_single%3D21042%26lat%3D39.276698%26lon%3D-76.899406%26geo_address%3DEllicott%2BCity%252C%2BMD%2B21042%26address_street_1%3D%26address_street_2%3D%26city%3DEllicott%2BCity%26state%3DMD%26zip%3D21042%26service%3DROUTINE_PHLEBOTOMY%26radius%3D25%26gps%3Dfalse
dr: https://www.labcorp.com/
ul: en-us
de: UTF-8
dt: Labcorp | PreCheck
sd: 24-bit
sr: 1440x900
vp: 563x733
je: 0
ec: Visit Info
ea: Food/Drink
el: Yes - Has had food/drink
_u: CACAAEABAAAAACAAI~
jid:
gjid:
cid: 1507150916.1694533203
tid: UA-96543265-1
_gid: 1478747976.1706632510
z: 285493723

Fig. 10

52. Finally, the patient is directed to complete a series of forms with personal, billing, and contact information, including their: first and last name, sex, date of birth, home address, insurance coverage (primary, secondary, out of pocket, etc...), and their primary insurance coverage plan.

53. Once the patient enters this information, Labcorp's Google Collection Tools intercept and transmit both the "contents" and "characteristics" of every communication the patient has entered into each text box including, among other things: the date and time of the appointment, the location of the appointment, the patient's gender, date of birth, and home address, their insurance coverage type, the name of their insurance provider, and several identifiers that uniquely identify the patient, such as the cid, tid, and _gid cookies. *See* Fig. 11(a)-(b).

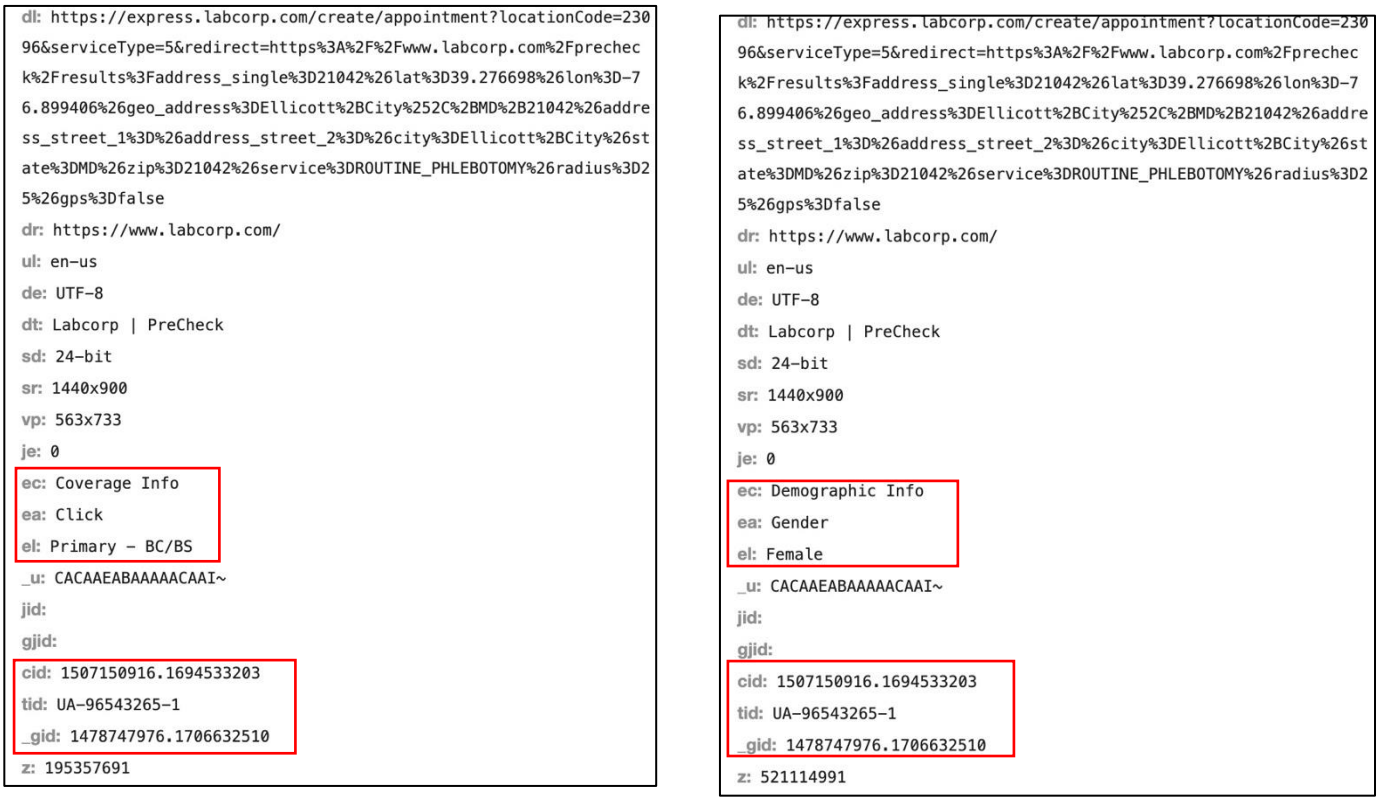
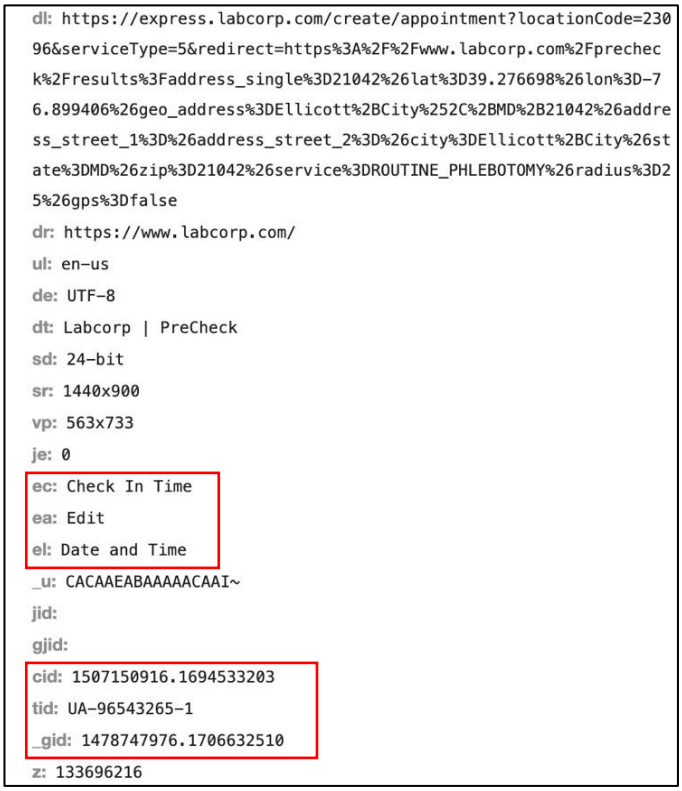
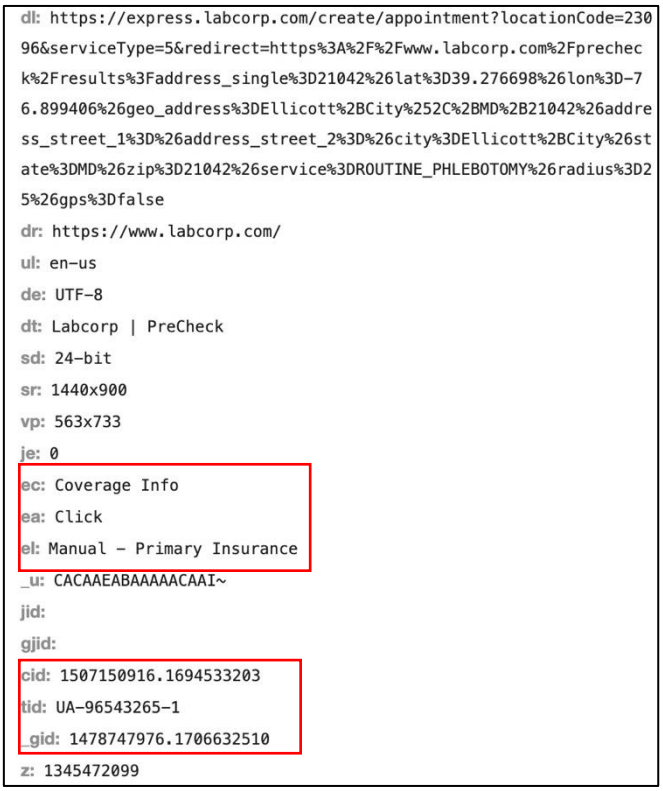


Fig. 11(a)


dl: https://express.labcorp.com/create/appointment?locationCode=23096&serviceType=5&redirect=https%3A%2F%2Fwww.labcorp.com%2Fprecheck%2Fresults%3Faddress_single%3D21042%26lat%3D39.276698%26lon%3D-76.899406%26geo_address%3DEllicott%2BCity%252C%2BMD%2B21042%26address_street_1%3D%26address_street_2%3D%26city%3DEllicott%2BCity%26state%3DMD%26zip%3D21042%26service%3DROUTINE_PHLEBOTOMY%26radius%3D25%26gps%3Dfalse
dr: https://www.labcorp.com/
ul: en-us
de: UTF-8
dt: Labcorp | PreCheck
sd: 24-bit
sr: 1440x900
vp: 563x733
je: 0
ec: Check In Time
ea: Edit
el: Date and Time
_u: CACAAEABAAAAACAAI~
jid:
gjid:
cid: 1507150916.1694533203
tid: UA-96543265-1
_gid: 1478747976.1706632510
z: 133696216


dl: https://express.labcorp.com/create/appointment?locationCode=23096&serviceType=5&redirect=https%3A%2F%2Fwww.labcorp.com%2Fprecheck%2Fresults%3Faddress_single%3D21042%26lat%3D39.276698%26lon%3D-76.899406%26geo_address%3DEllicott%2BCity%252C%2BMD%2B21042%26address_street_1%3D%26address_street_2%3D%26city%3DEllicott%2BCity%26state%3DMD%26zip%3D21042%26service%3DROUTINE_PHLEBOTOMY%26radius%3D25%26gps%3Dfalse
dr: https://www.labcorp.com/
ul: en-us
de: UTF-8
dt: Labcorp | PreCheck
sd: 24-bit
sr: 1440x900
vp: 563x733
je: 0
ec: Coverage Info
ea: Click
el: Manual - Primary Insurance
_u: CACAAEABAAAAACAAI~
jid:
gjid:
cid: 1507150916.1694533203
tid: UA-96543265-1
_gid: 1478747976.1706632510
z: 1345472099

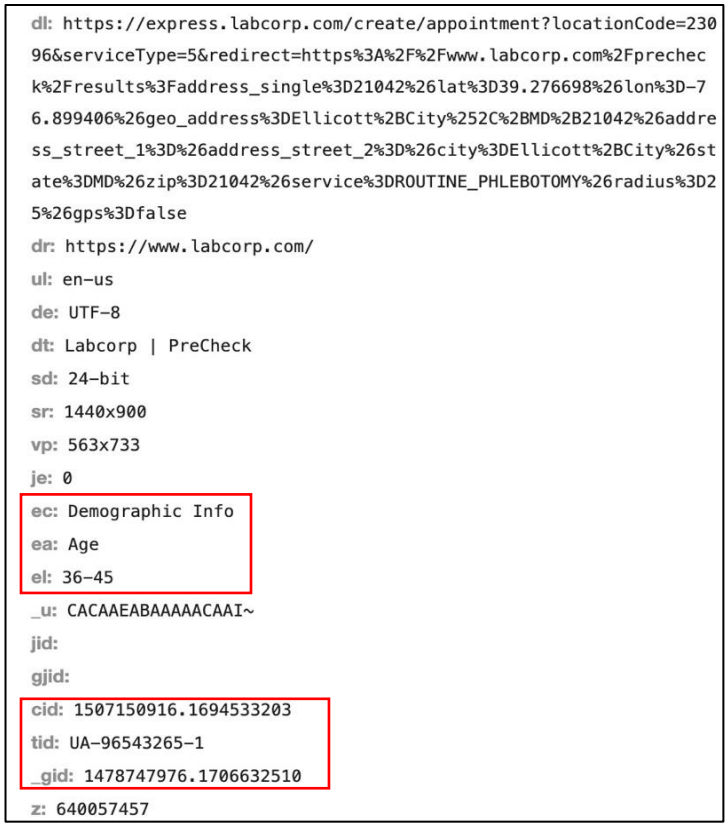

dl: https://express.labcorp.com/create/appointment?locationCode=23096&serviceType=5&redirect=https%3A%2F%2Fwww.labcorp.com%2Fprecheck%2Fresults%3Faddress_single%3D21042%26lat%3D39.276698%26lon%3D-76.899406%26geo_address%3DEllicott%2BCity%252C%2BMD%2B21042%26address_street_1%3D%26address_street_2%3D%26city%3DEllicott%2BCity%26state%3DMD%26zip%3D21042%26service%3DROUTINE_PHLEBOTOMY%26radius%3D25%26gps%3Dfalse
dr: https://www.labcorp.com/
ul: en-us
de: UTF-8
dt: Labcorp | PreCheck
sd: 24-bit
sr: 1440x900
vp: 563x733
je: 0
ec: Demographic Info
ea: Age
el: 36-45
_u: CACAAEABAAAAACAAI~
jid:
gjid:
cid: 1507150916.1694533203
tid: UA-96543265-1
_gid: 1478747976.1706632510
z: 640057457

Fig. 11(b)

54. However, the Google Collection Tools on Labcorp's website are not limited to collecting individually-identifiable health information related to, or gathered in the process of, scheduling test appointments. To the contrary, these tools gather all the data entered and created from every single patient interaction with the Labcorp website. For example, if a patient visits Labcorp's website and clicks on the "Diseases or Condition" tab, they are directed to a page, *https://www.labcorp.com/diseases*, showing 39 different diseases and conditions ranging from "Allergies" to "Women's wellness."

55. A patient who, clicks the "Overview" link from the "Kidney disease (chronic)" tab is directed to a page, *https://www.labcorp.com/chronic-kidney-disease*, that includes buttons and links providing information about specific treatment options, services, webinars, and tests, each with a separate link. Selecting any of these links, like "Your testing options for CKD" directs them to a new page, like *https://www.labcorp.com/chronic-kidney-disease/providers#tests*, that includes more buttons linked to specific kidney disease tests. Someone who clicks "Kidney Profile" is directed to an additional page, *https://www.labcorp.com/tests/140301/kidney-profile*, providing further information about kidney profile testing, and links to find and order a test.

56. Labcorp's Google Collection Tools intercept and transmit both the "contents" and "characteristics" of every communication the patient makes including, among other things: their advertising ID, cookie identifiers, and device identifiers. This is just one example of the hundreds (or thousands) of paths available on Defendant's website, and explains how Labcorp's use of Google Collection Tools enabled it to collect a wide array of individually-identifiable health information from every visitor to its website – including all the specific healthcare information they view – and share this information with Google.

57. After it receives the individually-identifiable health information from Labcorp's website, Google analyzes and uses this information for its own commercial purposes that include: building more fulsome profiles of its users' preferences and traits, and selling more-targeted advertisements based on this information. Google also receives an additional commercial benefit from Labcorp's use of Google's Collection Tools, namely that it provides Labcorp with a greater incentive to advertise on Google's platforms.

58. After it receives the individually-identifiable health information from its website and Google's analysis of this data, Labcorp uses this information for its own commercial purposes that include: understanding how people use its website and determining what ads people see on its website. Labcorp also receives an additional commercial benefit from using the Google Collection Tools, namely a substantial payment from Google for giving it access to the commercially-valuable, individually-identifiable health information communicated on its website.

59. Google is not any patient's intended recipient of individually-identifiable health information they communicate on Labcorp's website, nor is it an active or disclosed participant in these communications. Google only receives individually-identifiable health information from the Labcorp website by virtue of Labcorp's adoption of the Google Collection Tools.

60. Labcorp did not notify its website users that its website automatically shares individually-identifiable health information they communicate on its website to Google.

61. Labcorp did not notify its website users that Google is using individually-identifiable health information they communicate on its website for commercial purposes.

62. Labcorp did not notify its website users that it is using the individually-identifiable health information they communicate on its website for its own commercial purposes.

63. Google did not secure informed consent or express written authorization allowing it to use individually-identifiable health information communicated on Labcorp's website for commercial, or any, purposes.

64. Labcorp did not secure informed consent or express written authorization allowing it to share individually-identifiable health information communicated on its website with Google.

65. Labcorp did not secure informed consent or express written authorization allowing it to use individually-identifiable health information communicated on its website for commercial purposes.

66. All these facts establish that Labcorp's actions clearly violated its own privacy policies by, at a minimum:

a. Misrepresenting that it would protect and ensure the confidentiality of its website visitors' individually-identifiable health information;

b. Misrepresenting that it would seek explicit consent before collecting individually-identifiable health information from its website visitors;

c. Misrepresenting that it would seek and secure website visitors' authorization before using or disclosing their individually-identifiable health information for profit;

d. Misrepresenting that its website would not collect individually-identifiable health information from visitors;

e. Misrepresenting that it would obtain personally-identifying information from website visitors only if they "voluntarily choose to provide such information via correspondence;"

f. Misrepresenting that it only used Google Analytics to "analyze traffic" to the various Labcorp webpages, and not for any other purpose;

g. Misrepresenting that its website only collected data regarding "site usage" from visitors, and not any other type of data;

h. Misrepresenting that its website only compiled visitors' "site usage" data "in the aggregate," as opposed to compiling this data on an individual basis;

i. Misrepresenting that its website collected visitors' "site usage" data only "to improve the performance of the site, create a profile of uses, and improve our marketing and advertisements," and not for any other purpose.

Labcorp Falsely Promises That Patients Can Opt-Out of Third-Party Tracking Tools

67. Labcorp's Website ostensibly provides its users with an option to disable third party cookies and tracking tools under the "Manage Cookies" link posted on the website's homepage. *See* Fig. 12.

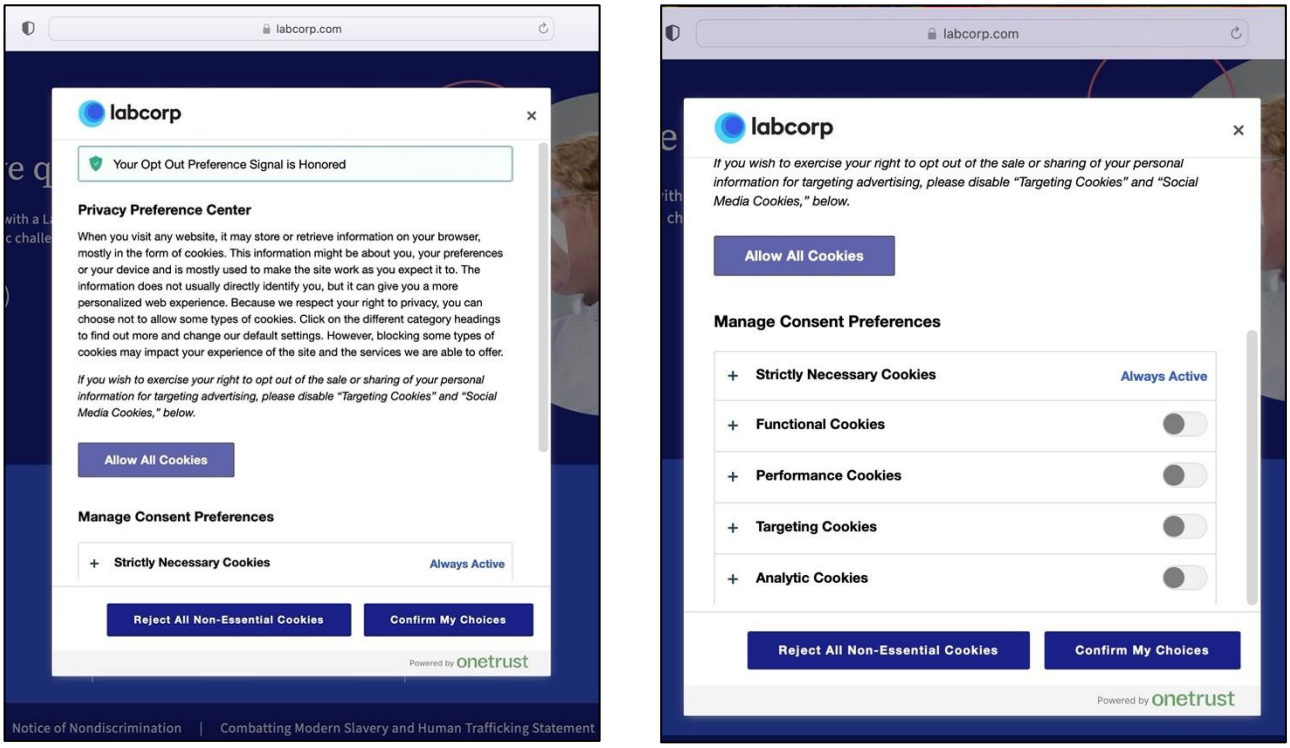


Fig. 12

68. As displayed above, when a Labcorp website user opts to disable some or all its cookies, the Labcorp website displays a message promising: "Your Opt Out Preference Signal is Honored." *Id.*

69. In truth, however, even if a Labcorp website user disables all their cookies through this process, their preferences do not override or delete Labcorp's Google Collection Tools. To the contrary, these tools remain active and continue to intercept and disclose the contents and characteristics of that user's individual communications as they navigate through the website without regard for their preference settings.

Named Plaintiffs' Interactions With Labcorp's Website

70. Between early 2022 and March 8, 2023, Michael Wiggins used the Labcorp website to research [redacted] testing options and locations, schedule a [redacted] test, and view his test results. The full extent of Labcorp's interception and disclosure of Mr. Wiggins' communications to Google can only be determined through formal discovery. However, the Google Collection Tools on Labcorp's website intercepted and sent to Google at least the following URLs, or substantially similar URLs, including individually-identifiable health information from Mr. Wiggins' interactions of logging into Labcorp's patient portal and scheduling his [redacted] test:

a. *https://patient.labcorp.com/*;

b. *https://www.labcorp.com/frequently-asked-questions/patient/labs-appointments/all*;

c. *https://www.labcorp.com/frequently-asked-questions/patient/labcorp-patient-portal/test-results*;

d. *https://www.labcorp.com/frequently-asked-questions/patient/labcorp-patient-portal/test-results#:~:text=access%20my%20lab%20test-,results,-%3F*;

e. *https://www.labcorp.com/frequently-asked-questions/patient/labcorp-patient-portal/test-results#:~:text=lab%20test%20results-,%3F,-Still%20need%20help*;

f. [redacted]; and

g. [redacted]

[redacted].

71. When Mr. Wiggins scheduled his [redacted] test appointment on Labcorp's website, Google Collection Tools intercepted and sent to Google the required individually-identifiable health information he entered in the electronic forms as shown in ¶¶ 43-53, above. This information includes, but is not limited to: his home address, the type of test or service he scheduled, the date, time, and location of his appointment, whether he was fasting before the appointment, his gender, age, and the name of his insurance provider.

72. Every time Mr. Wiggins used the Labcorp website during the relevant period, the Google Collection Tools intercepted and sent to Google both the "characteristics" of his communications with Labcorp (including his personal advertising ID, cookie identifiers, device identifiers, and account numbers) and the "content" of these communications (including the information he entered into text boxes and every URL, button, link, page, and tab he clicked or viewed on the site), all of which constitute individually-identifiable health information.

73. Labcorp never notified Mr. Wiggins that it would share his individually-identifiable health information with Google, put this information to its own commercial use, or allow Google (or any other third party) to put this information to any commercial use.

74. Mr. Wiggins never consented to allow Labcorp to share his individually-identifiable health information with Google, put this information to its own commercial use, or allow Google (or any other third party) to put this information to any commercial use.

75. Nevertheless, Labcorp shared Mr. Wiggins' individually-identifiable health information with Google, put this information to its own commercial use, and allowed Google to

use this information to serve Mr. Wiggins focused ads concerning [redacted]-related products like [redacted] and several [redacted] testing kits through banner ads on several websites.

76. Between early 2022 and March 8, 2023, Plaintiff Teri Stevens used the Labcorp website to research [redacted] testing options and locations, schedule a [redacted] test, and view her test results. The full extent of Labcorp's interception and disclosure of Ms. Stevens' communications to Google can only be determined through formal discovery. However, the Google Collection Tools on Labcorp's website intercepted and sent to Google at least the following URLs, or substantially similar URLs, including individually-identifiable health information from Ms. Stevens' interactions of logging into the Labcorp patient portal and scheduling a [redacted] test:

a. *https://patient.labcorp.com/*; and

b. [redacted].

77. When Ms. Stevens scheduled her [redacted] test appointment on Labcorp's website, Google Collection Tools intercepted and sent to Google the required individually-identifiable health information she entered in the electronic forms as shown in ¶¶ 43-53, above. This information includes, but is not limited to: her home address, the type of test or service she scheduled, the date, time, and location of her appointment, whether she was fasting before the appointment, her gender, age, and the name of her insurance provider.

78. Every time Ms. Stevens used the Labcorp website during the relevant period, the Google Collection Tools intercepted and sent to Google both the "characteristics" of her communications with Labcorp (including her personal advertising ID, cookie identifiers, device

identifiers, and account numbers) and the "content" of these communications (including the information she entered into text boxes and every URL, button, link, page, and tab she clicked or viewed on the site), all of which constitute individually-identifiable health information.

79. Labcorp never notified Ms. Stevens that it would share her individually-identifiable health information with Google, put this information to its own commercial use, or allow Google (or any other third party) to put this information to any commercial use.

80. Ms. Stevens never consented to allow Labcorp to share her individually-identifiable health information with Google, put this information to its own commercial use, or allow Google (or any other third party) to put this information to any commercial use.

81. Nevertheless, Labcorp shared Ms. Stevens' individually-identifiable health information with Google, put this information to its own commercial use, and allowed Google to use this information to serve Ms. Stevens focused ads concerning [redacted]-related products through banner ads on several websites.

DEFENDANT'S CONDUCT VIOLATES APPLICABLE PRIVACY LAWS

The HIPPA Privacy Rule Protects Patient Healthcare Information

HIPAA and its implementing regulations are meant to protect patient healthcare information. The HIPAA Privacy Rule, 45 C.F.R. § 160 and 45 C.F.R. §§ 164 (A) and (E), "establishes national standards to protect individuals' medical records and other individually-identifiable health information (collectively defined as 'protected health information') and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically."[39]

[39] *See* HHS.gov, Health Information Privacy (Mar. 31, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.*

83. The HIPAA Privacy Rule broadly defines "protected health information" ("PHI") as "individually-identifiable health information" ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." *See* 45 C.F.R. § 160.103.

84. HIPAA defines "IIHI" as "a subset of health information, including demographic information collected from an individual [that is] created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse, [r]elates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and either identifies the individual or [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." *See* 45 C.F.R. § 160.103.

85. Under the HIPAA de-identification rule: "health information is not individually-identifiable only if: an expert determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information [and] documents the methods and results of the analysis that justify such determination [or] the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

a. Names;

b. Medical record numbers;

c. Account numbers;

d. Device identifiers and serial numbers;

e. Web Universal Resource Locators (URLs);

f. Internet Protocol (IP) address numbers; … and

> g. Any other unique identifying number, characteristic, or code…; and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is subject of the information." 45 C.F.R. § 164.514.

86. The HIPAA Privacy Rule requires any "covered entity," including healthcare providers like Labcorp, to maintain appropriate safeguards to protect the privacy of protected health information, and sets clear limits and conditions on the uses and disclosures of protected health information without authorization. *See* 45 C.F.R. §§ 160.103, 164.502.

87. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "uses or causes to be used a unique health identifier, or obtains individually-identifiable health information relating to an individual." Under HIPAA, a "person… shall be considered to have obtained or disclosed individually-identifiable health information… if the information is maintained by a covered entity… and the individual obtained or disclosed such information without authorization." *See* 42 U.S.C. § 1320(d)(6).

88. Under HIPAA, it is a crime for any person to knowingly: use or cause to be used a unique health identifier; obtain individually identifiable health information relating to an individual; or disclose individually identifiable health information to another person. *See* 42 U.S.C. § 1320(d)(6).

HIPAA Protects Patient Status Information

89. Guidance from HHS confirms that HIPAA also protects an individual's status as a patient of a healthcare provider:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.… *If such information was listed with health condition,*

> *healthcare provision or payment data, such as an indication that an individual was treated at a certain clinic, then this information would be PHI.*[40]

90. HHS has repeatedly instructed that the HIPAA privacy Rule protects patient status.

For example:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA, 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list, 67 Fed. Reg. 53186 (Aug. 14, 2002);

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers," 78 Fed. Reg. 5642 (Jan. 25, 2013); and

d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient, 45 C.F.R. § 164.510(2).

91. HHS's guidance for marketing communications states that healthcare providers may not provide patient lists for marketing purposes without the consent of every included patient:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing… Simply put, a covered entity may not sell protected

[40] *See* Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (emphasis added) (Nov. 26, 2012), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhsdeidguidance.pdf*.

> health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining* authorization from each person on the list.[41]

Internet Marketing Activities Are Not Exempt From HIPAA Protection

92. In December 2022, HHS issued a Bulletin "to highlight the obligations" of healthcare providers and their business associates under the HIPAA Privacy Rule "when using online tracking technologies," such as the Google Collection Tools, that "collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application."[42]

93. The December 2022 HHS Bulletin confirmed that HIPAA applies to healthcare providers' use of tracking technologies like the Google Collection Tools.[43] Among other things, HHS explained that healthcare providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information even if no treatment information is included and even if the individual does not have a relationship with the healthcare provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually-identifiable health information (IIHI) that the individual providers

[41] *See* Office for Civil Rights, *Marketing* at 1-2 (emphasis added) (Apr. 3, 2003), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.*

[42] *See* HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information (Dec. 1, 2022), *https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html.*

[43] *See* Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (Dec. 1, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa- online-tracking/index.html.*

> when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of healthcare services. *This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e. it is indicative that the individual has received or will receive healthcare services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or healthcare or payment for care.*[44]

94. The December 2022 HHS Bulletin further explained that tracking technologies on healthcare providers' patient portals "generally have access to PHI" and may access diagnosis and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. *Tracking technologies on a regulated entity's user-authenticate webpages generally have access to PHI***.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. *Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal.* Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.[45]

[44] *Id.*

[45] *Id.*

95. The December 2022 HHS Bulletin reminded healthcare providers that HIPAA applies to the use of tracking technologies on unauthenticated webpages, *not just to patient portals*:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal ***… [and pages] that address[] specific symptoms or health conditions,*** such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering *credentials may have access to PHI in certain circumstances*. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[46]

96. As a result, the December 2022 HHS Bulletin explained that healthcare providers may not disclose PHI to a tracking technology vendor, like Google, unless it has properly notified its website users and entered into a business associate agreement with the vendor:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does *not* permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI. If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individual's HIPAA-compliant authorizations are required *before* the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of

[46] *Id.*

> tracking technologies, such as cookies, do *not* constitute a valid HIPAA authorization. [I]t is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place *and* requires that there is an applicable Privacy Rule permission for disclosure.[47]

97. All the concerns, obligations, and prohibitions discussed in the December 2022 HHS Bulletin are based on long-standing rules and guidance, in place for decades, that both Labcorp and Google were aware of and required to follow. *See Id.*

The FTC Act Protects Patient Healthcare Information

98. In the context of this case, the FTC has made clear that "health information" is "anything that conveys information – or enables an information – about a consumer's health" (like information about trips to a cancer treatment facility) "may convey highly sensitive information about a consumer's health." Jillson, Elisa, *Protecting The Privacy Of Health Information: A Baker's Dozen Takeaways From FTC Cases*, Federal Trade Commission (July 25, 2023), *https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers -dozen-takeaways-ftc-cases.*

99. The FTC has joined HHS in notifying HIPAA-covered entities (and non-HIPAA-covered entities) that sharing "health information" with "hidden third parties," like Google, constitutes an unfair business practice under federal law:

> When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health

[47] *Id.*

information from potential misuse and exploitation."[48]

Pennsylvania Law Protects Patient Healthcare Information

100. 28 Pa. Code § 115.27 provides that: all medical records and information: "shall be treated as confidential. Only authorized personnel shall have access to the records. The written authorization of the patient shall be presented and then maintained in the original record as authority for release of medical information outside the hospital."

101. Thus, Pennsylvania law requires all medical providers, including Labcorp, to maintain all medical records and information within their control as confidential, rendering Labcorp's actions with respect to the interception and disclosure of its patients' health communications to Meta unlawful under Pennsylvania law.

Patients Have A Protectable Property Interest In Their Individually-Identifiable Health Information

102. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications. Plaintiffs and the Class members have a vested property right in their individually-identifiable health information.

103. Courts have described the concept of "property" broadly:

a. "property," as used in the Constitution, is a word of most general import and extends to every species of right and interest, capable of being enjoyed as such, upon which it is practicable to place a money value, *see Council Rock Sch. Dist. v. Land in Northampton Tp.*, 46 Pa. D. & C.2d 245, 248–49 (Pa. Com. Pl. 1968), *quoting* 26 Am. Jur. 2d, Eminent Domain, §173, p. 848 (1966);

b. *The Chesapeake and Ohio Ry. Co. v. Burkentine*, 45 Pa. D. & C.3d 344, 347 (Pa. Com. Pl. 1987) (describing property as "everything that has exchangeable value");

[48] *See* FTC and HHS Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies, Federal Trade Commission (July 20, 2023), *https:// www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking*.

c. Also included in the bundle of rights constituting "property" is the right to exclude other persons from using the thing in question, *see Pet. of Borough of Boyertown*, 466 A.2d 239, 245 (Pa. Cmmw. 1983), *citing Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419 (1982).

104. Federal and state law both grant patients the right to protect the confidentiality of data that identifies them as patients of a particular healthcare provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

105. A patient's right to protect the confidentiality of his or her health data and restrict others' access to this data is valuable.

106. In addition, patients enjoy property rights in the privacy of their health communications under statutes such as HIPAA; and 28 Pa. Code § 115.27. Federal and state courts have long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

107. Property rights in communications and information privacy are established by:

a. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored Communications Act); and Title III (the Pen Register Act);

b. State laws, including 28 Pa. Code § 115.27; and

c. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist, s*ee Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

108. Labcorp's unauthorized interception and disclosure of Plaintiffs' and the Class members' individually-identifiable health information violated their property rights to control how

their data and communications are used and who may be the beneficiaries of their data and communications.

The Individually-Identifiable Health Information Labcorp Disclosed To Google Has Measurable Monetary Value

109. Google generates nearly 80% of its annual revenue from advertising.[49]

110. In addition to its own independent marketing programs, Google also receives billions of dollars of unearned advertising sales revenue from Google healthcare partners, including Labcorp, who are targeting Google users based on their health information.

111. Courts recognize the value of personal information and the harm when it is disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

112. Healthcare data is particularly valuable on the black market because it often contains all an individual's PII and medical conditions as opposed to a single piece of information that, for example, is ordinarily stolen in a financial breach.

113. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

[49] Abigail Bosze, Google Revenue Breakdown (2024), *https://www.doofinder.com/en/statistics/google-revenue-breakdown*; James Ball, Online Ads Are About to Get Even Worse, The Atlantic (June 1, 2023) *https://www.theatlantic.com/technology/archive/2023/06/advertising-revenue-google-meta-amazon-apple-microsoft/674258/.*

114. The value of health data is well-known and various reports have been conducted to identify its value.

115. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[50]

116. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[51]

117. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[52]

118. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[53]

---

[50] *See https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf* (last visited Jan. 9, 2024).

[51] *See https://www.imprivata.com/blog/healthcare-data-new-prize-hackers* (last visited Jan. 9, 2024), *citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf*).

[52] *See https://time.com/4588104/medical-data-industry/* (last visited Jan. 9, 2024).

[53] *See https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html* (last visited Jan. 9, 2024).

119. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

120. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

121. Google's and others' practices of using such information to package groups of people as "Lookalike Audiences" and similar groups and selling those packages to advertising clients demonstrates the financial worth of that data. Data harvesting is the fastest growing industry in the nation.

122. As software, data mining and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

123. Consumer data is so valuable that some have proclaimed that data is the new oil.

124. Between 2016 and 2018, the value of information mined from Americans increased by 40% for Google.

125. Overall, the value internet companies derive from Americans' personal data increased by almost 54% from 2016 to 2018, and is only expected to continue growing in the coming years.

126. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user. By 2020, that value had jumped to approximately $420 per adult American user each year, making personal data sales a nearly $140 million industry.[54]

[54] Medium, How Much Is User Data Worth?, Mar. 16, 2020, *https://pawtocol.medium.com/how-much-is-user-data-worth-f2b1b0432136* (last visited Jan. 26, 2024); Invisibly, How Much Is Your Data Worth? The Complete Breakdown For 2024, July 13, 2021, *https://www.invisibly.com/learn-blog/how-much-is-data-worth/#:~:text=Together%2C%20internet%20advertising%20turned%20%24139.8,back%20of%20your%20personal%20data* (last visited Jan. 26, 2024).

127. In 2025, that value is expected to exceed $225 billion industry-wide.[55]

128. As to health data specifically, as detailed in an article in Canada's National Post:

> As part of the multibillion-dollar worldwide data brokerage industry, health data is one of the most sought-after commodities. De-identified data can be re identified (citing https://www.nature.com/articles/s41467-019-10933-3/) and brazen decisions to release records with identifiable information (citing https://www.wsj.com/articles/hospitals-give-tech-giants-access-todetailed-medical-records-11579516200?mod=hp_lista_pos3) are becoming commonplace).[56]

129. Further demonstrating the financial value of Class Members' medical data, CNBC has reported that hospital executives have received a growing number of bids for user data:

> Hospitals, many of which are increasingly in dire financial straits, are weighing a lucrative new opportunity: selling patient health information to tech companies. Aaron Miri is chief information officer at Dell Medical School and University of Texas Health in Austin, so he gets plenty of tech start-ups approaching him to pitch deals and partnerships. Five years ago, he'd get about one pitch per quarter. But these days, with huge data-driven players like Amazon and Google making incursions into the health space, and venture money flooding into Silicon Valley start-ups aiming to bring machine learning to health care, the cadence is far more frequent. "It's all the time," he said via phone. "Often, once a day or more."
>
> * * *
>
> [H]ealth systems administrators say [the data] could also be used in unintended or harmful ways, like being cross-referenced with other data to identify individuals at higher risk of diseases and then raise their health premiums, or to target advertising to individuals.[57]

---

[55] Invisibly, Top Industries And Companies That Sell Your Data, Aug. 20, 2021, *https://www.invisibly.com/learn-blog/companies-selling-your-personal-data/* (last visited Jan. 26, 2024).

[56] *See* National Post, Iris Kulbatski: The Dangers Of Electronic Health Records, Feb. 26, 2020, *https://nationalpost.com/opinion/iris-kulbatski-the-dangers-of-electronichealth-records* (last visited Aug. 15, 2023).

[57] CNBC, Hospital Execs Say They Are Getting Flooded With Requests For Your Health Data, *https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html* (last visited Aug. 15, 2023).

130. The CNBC article also explained:

> De-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers. Just one company alone, IQVIA, said on its website that it has access to more than 600 million patient records globally that are nonidentified, much of which it accesses through provider organizations. The buyers, which include pharma marketers, will often use it for things like clinical trial recruiting But hospital execs worry that this data may be used in unintended ways, and not always in the patient's best interest.

131. Tech companies are also under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own needs. For instance, the health data Google collects could eventually help it micro-target advertisements to people with particular health conditions. Policymakers are proactively calling for a revision and potential upgrade of the health privacy rules known as HIPAA, out of concern for what might happen as tech companies continue to march into the medical sector.[58]

132. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

133. The unauthorized possession and use of Plaintiffs' and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Website Users, including Plaintiffs and Class Members.

134. Plaintiffs have a continuing interest in ensuring that their future communications with Labcorp are protected and safeguarded from future unauthorized disclosure.

---

[58] *Id.*

CLASS ACTION ALLEGATIONS

135. Plaintiffs bring this action as a class action under Federal Rules of Civil Procedure 23(a) and (b)(3) for:

> All persons whose protected health information was disclosed to Google without authorization or consent through the Google Collection Tools on Labcorp's website before March 8, 2023 ("the Class members").[59]

136. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(1), because the Class members are so numerous and geographically-dispersed that their joinder would be impracticable. Plaintiffs believe that Defendant's and Google's business records will permit the identification of thousands of people meeting the Class definition.

137. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(2), because there are many common questions of facts and law concerning and affecting the Class members, including:

a. Whether Labcorp had a duty to protect and refrain from disclosing the Class members' individually-identifiable health information;

b. Whether Labcorp intentionally disclosed the Class members' individually-identifiable health information to Google;

c. Whether the Class members consented to Labcorp's disclosure of their individually-identifiable health information to Google;

d. Whether the Class members are entitled to damages because of Labcorp's conduct; and

e. Whether Labcorp's knowing disclosure of its patients' individually-identifiable health information to Google involves "criminal or tortious" conduct under 18 U.S.C. § 2511(2)(d).

138. Plaintiffs also anticipate that Defendant will raise defenses common to the Class.

[59] Plaintiffs include a date limitation for their proposed Class in consideration of a March 8, 2023 update adding arbitration and class waiver provisions to Labcorp's website Terms and Conditions.

139. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(3), because Plaintiffs' claims are typical of the claims belonging to the Class members. Plaintiffs and the Class members were harmed by the same wrongful conduct perpetrated by Defendant that caused their individually-identifiable health information to be intercepted and disclosed without notice or consent. As a result, Plaintiffs' claims are based on the same facts and legal theories as the Class members' claims.

140. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(4), because Plaintiffs will fairly and adequately protect the interests of all the Class members, there are no known conflicts of interest between Plaintiffs and the Class members, and Plaintiffs have retained counsel experienced in the prosecution of complex litigation.

141. Class certification is appropriate under Fed. R. Civ. P. 23(b)(3), because common questions of law and fact predominate over questions affecting the individual Class members, because a class action is superior to other available methods for the fair and efficient adjudication of these claims and because important public interests will be served by addressing the matter as a class action. Further, the prosecution of separate actions by the individual Class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and substantially impair the Class members' ability to protect their interests.

COUNT I
Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*

142. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

143. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. *See* 18 U.S.C. § 2511.

144. The ECPA provides a private right of action to any person whose electronic communications are intercepted. *See* 18 U.S.C. § 2520(a).

145. The ECPA protects both the sending and receiving of communications. *See* 18 U.S. Code § 2511(1)(a); 18 U.S. Code § 2510(12).

146. The transmissions of data between Plaintiffs and the Class members, on one hand, and Labcorp and Google, on the other, qualify as "communications" under the ECPA. *See* 18 U.S.C. § 2510(12).

147. The following constitute "devices" under the ECPA:

a. the cookies Labcorp and Google use to track Plaintiffs' and the Class members' communications;

b. Plaintiffs' and the Class members' browsers;

c. Plaintiffs' and the Class members' computing devices;

d. Labcorp's web-servers or webpages where the Google Collection Tools are present;

e. Google's web-servers; and

f. the Google Collection Tools source code Labcorp deploys on its website to acquire Plaintiffs' and the Class members' communications.

See 18 U.S.C. § 2510(5).

148. Labcorp received electronic communications Plaintiffs and the Class members made on Labcorp's website using Google Collection Tools and intentionally and surreptitiously transmitted these communications to Google.

149. The illegally-transmitted communications supporting Plaintiffs' claims include information communicated when Plaintiffs and the Class members:

a. log-in to the Labcorp website;

b. schedule an appointment on the Labcorp website;

c. search for a test location on the Labcorp website;

d. select a test location on the Labcorp website;

e. make a test appointment on the Labcorp website;

f. enter information into text boxes on the Labcorp website;

g. visit or move between pages on the Labcorp website; or

h. click buttons, links, or tabs on the Labcorp website.

150. For example, Defendant's interception of the fact that Plaintiffs viewed a webpage like [redacted] involves "content," because it communicated Plaintiffs' request for the information on that page.

151. Labcorp did not notify Plaintiffs or the Class members that it intended to share individually-identifiable health information they communicated on its website with Google, and Plaintiffs and the Class members did not authorize or consent to any such sharing.

152. Labcorp did not notify Plaintiffs or the Class members that it intended to use individually-identifiable health information they communicated on its website for commercial purposes, and Plaintiffs and the Class members did not authorize or consent to any such use.

153. Labcorp's disclosure of Plaintiffs' and the Class members' individually-identifiable health information to Google without their notice and consent or authorization violated the ECPA, because this disclosure violates HIPAA.

154. Labcorp's acquisition and disclosure of Plaintiffs' and the Class members' individually-identifiable health information "with intent to sell, transfer, or use" it for "commercial advantage [or] personal gain" violated the ECPA, because these actions violate HIPAA.

155. Labcorp's disclosure of Plaintiffs' and the Class members' individually-identifiable health information to Google without notice and consent or authorization violated the ECPA,

because these actions violate 18 U.S.C. §§ 1343 and 1349 (federal wire fraud statutes prohibiting a person from devising a scheme to defraud, or obtaining money or property by means of false or fraudulent pretenses, representations or promises, or transmitting communications by wire in interstate commerce to execute such a scheme).

156. Labcorp's disclosure of Plaintiffs' and the Class members' individually-identifiable health information to Google for commercial purposes without notice and consent or authorization violated the ECPA, because these actions violate 28 Pa. Code § 115.27 (prohibiting healthcare providers from sharing health care information, medical records, and related information with third parties).

157. Labcorp's disclosure of Plaintiffs' and the Class members' individually-identifiable health information to Google for commercial purposes without notice and consent or authorization violated the ECPA, because these actions constituted a breach of contract. *See* Count II, below.

158. Labcorp's disclosure of Plaintiffs' and the Class members' individually-identifiable health information to Google for commercial purposes without notice and consent or authorization violated the ECPA, because these actions constitute negligence. *See* Count III, below.

159. Labcorp's disclosure of Plaintiffs' and the Class members' individually-identifiable health information to Google for commercial purposes without notice and consent or authorization violated the ECPA, because these actions constitute a violation of privacy laws. *See* Count IV, below.

160. Labcorp's disclosure of Plaintiffs' and the Class members' individually-identifiable health information to Google for commercial purposes violated the ECPA, because these actions caused Labcorp to be unjustly enriched. *See* Count V, below.

161. Plaintiffs and the Class members have been harmed by Labcorp's violations of the ECPA, so are entitled to recover all statutory damages provided by 18 U.S.C. § 2520.

COUNT II
Breach of Contract

162. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

163. During the relevant period, Labcorp's website Terms and Conditions provided: "Our Privacy Statement and, with respect to protected health information, our Notice of Privacy Practices describe how Labcorp collects information about you through the Online Services, and how we use, disclose, and protect that information." Labcorp Terms and Conditions, *https://www.labcorp.com/terms-and-conditions* (Sept. 30, 2021).

164. Labcorp's Notice of Privacy Practices and Web Privacy Statement make several express promises about its receipt, handling, and use of patients' health information, including that:

a. "Labcorp is required by law to maintain the privacy of health information that identifies you, called protected health information (PHI)… Labcorp is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation. We take this commitment seriously...," Labcorp's Notice of Privacy Practices, *https://www.labcorp.com/about/hipaa-information* (Jan. 31, 2020);

b. For… uses and disclosures of PHI for marketing purposes and disclosures that would constitute a sale of PHI, Labcorp will ask for patient authorization before using or disclosing PHI," *id*.;

c. "We do not ask You to provide personal health care information to Us through our general website. We obtain personally identifying information about You only if You voluntarily choose to provide such information via correspondence with Us," Labcorp Web Privacy Statement, *https://www.labcorp.com/about/web-privacy-policy* (Nov. 27, 2023); and

d. Labcorp will seek "explicit consent" before collecting "sensitive personal information (such as your… health information)," *id.*

165. As described throughout this filing, Labcorp breached these express promises it made to Plaintiffs and the Class members in many ways, including by:

a. sharing patient portal login information with Google for commercial purposes without notice or consent;

b. disclosing patient advertising IDs, cookie identifiers, and device identifiers to Google for commercial purposes without notice or consent; and

c. disclosing the content of patient communications containing individually-identifiable health information to Google for commercial purposes without notice or consent.

166. Plaintiffs and the Class Members have suffered damages from Labcorp's breaches of contract that include, among other things:

a. the loss in value of their individually-identifiable health information, or their property rights in this information, resulting from the unauthorized use of this information, including by Labcorp and Google; and

b. the loss in value of the medical services they received, which included promises to maintain the confidentiality of their individually-identifiable health information and not to share or use this information for commercial purposes.

COUNT III
Negligence

167. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

168. Plaintiffs and the Class members have communicated individually-identifiable health information to Labcorp through its website and/or received healthcare services from Labcorp's employees.

169. By virtue of creating and maintaining its website as a public healthcare resource and its employment of those individuals who provided Plaintiffs and the Class members with

healthcare services, Labcorp assumed a duty to keep confidential all individually-identifiable health information Plaintiffs and the Class members communicated.

170. Labcorp assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable health information confidential, protected, and private by issuing a Notice of Privacy Practices representing that: "Labcorp is required by law to maintain the privacy of health information that identifies you, called protected health information (PHI)…" *See* Labcorp's Notice of Privacy Practices, *https://www.labcorp.com /about/hipaa-information* (Jan. 31, 2020).

171. Labcorp assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable health information confidential, protected, and private by issuing a Notice of Privacy Practices representing that: "Labcorp is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation. We take this commitment seriously..." *Id.*

172. Labcorp assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable health information confidential, protected, and private by issuing a Notice of Privacy Practices representing that: "For… uses and disclosures of PHI for marketing purposes and disclosures that would constitute a sale of PHI, Labcorp will ask for patient authorization before using or disclosing PHI." *Id.*

173. Labcorp assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable health information confidential, protected, and private by issuing a Web Privacy Statement representing that: "We do not ask You to provide personal health care information to Us through our general website. We obtain personally identifying information about You only if You voluntarily choose to provide such information via correspondence with Us." Labcorp Web Privacy Statement, *https://www.labcorp.com/about/web-privacy-policy* (Nov. 27, 2023).

174. Labcorp assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable health information confidential, protected, and private by issuing a Web Privacy Statement representing that: it would seek "explicit consent" before collecting "sensitive personal information (such as your… health information)." *Id.*

175. Labcorp has a legal duty not to disclose Plaintiffs' and the Class members' medical records for marketing purposes without their express written authorization under multiple federal laws. *See, e.g.*, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

176. Labcorp has a legal duty to keep Plaintiffs' and the Class members' medical records confidential and private absent express written authorization under Pennsylvania law. *See, e.g.*, 28 Pa. Code § 115.27.

177. Labcorp breached the various duties of care it owes and assumed by, among other things: placing computer code on its website that intercepts the characteristics and content of communications about individually-identifiable health information; automatically transmitting this data to Google; putting this data to its own commercial use; allowing Google to put this data to its own commercial use; failing to provide adequate notice to Plaintiffs or the Class members of any of these activities, and failing to receive Plaintiffs' or the Class members' informed consent to engage in any of these activities.

178. Plaintiffs and the Class members have suffered damages because of Labcorp's negligence that include, among other things:

a. the loss in value of their individually-identifiable health information, or their property rights in this information, resulting from the unauthorized use of this information, including by Labcorp and Google; and

b. the loss in value of the medical services they received, which included promises to maintain the confidentiality of their

individually-identifiable health information and not to share or use this information for commercial purposes.

179. Labcorp proximately caused the damages identified above by intentionally and willfully engaging in the acts that caused Plaintiffs' and the Class members' individually-identifiable health information to be shared with Google, allowing Google to put this information to commercial use, and putting this information to its own commercial use without providing adequate notice to Plaintiffs or the Class members of any of these activities, or receiving their informed consent to engage in any of these activities.

COUNT IV
Invasion of Privacy - Intrusion Upon Seclusion

180. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

181. By collecting and disseminating the content of Plaintiffs' and the Class members' communications without their knowledge, Labcorp intentionally intruded into Plaintiffs' and the Class members' private affairs or concerns.

182. The communications at issue include Plaintiffs' and the Class members' patient portal logins and communications regarding conditions, treatments, symptoms, payments, and other health-related content.

183. Plaintiffs and the Class members enjoyed an objectively-reasonable expectation of privacy in their communications with Labcorp's website based on:

a. Labcorp's status as their healthcare provider and the reasonable expectations of privacy that attach to patient-provider relationships;

b. Provisions in the HIPAA that protect individually-identifiable health information;

c. Provisions in the ECPA that protect individually-identifiable health information;

d. Pennsylvania's medical privacy laws;

e. Labcorp's many express promises that its website was a private and protected environment for communicating individually-identifiable health information and that it would keep this information private and not share it for commercial purposes without notice and express consent; and

f. The widely-accepted consensus in modern American society that individual patients' medical information is, and includes, sensitive information that cannot be shared with third parties without notice and consent, demonstrated by public polling that shows: "[n]inety-seven percent of Americans believe that doctors, hospitals, labs, and health technology systems should not be allowed to share or sell their sensitive health information without consent.[60]

184. Labcorp's intrusion into Plaintiffs' and the Class members' privacy was highly offensive to a reasonable person, because it violated HIPAA and represented conduct inconsistent with the December 2022 HHS Bulletin, violated protections for healthcare information in the FTC Act and Pennsylvania law, violated the ECPA, constituted a breach of contract and negligence, violated their privacy and property rights, and caused Labcorp to be unjustly enriched.

185. Labcorp's intrusion into Plaintiffs' and the Class members' privacy is highly offensive to a reasonable person, because it was carried out with the intent to knowingly derive a financial benefit from use of private, confidential medical information.

186. Labcorp's intrusion into Plaintiffs' and the Class members' privacy is highly offensive to a reasonable person, because it was intentionally carried out in a surreptitious manner, concealed from Plaintiffs and the Class members, and without their knowledge or consent.

187. Plaintiffs and the Class members have suffered damages from Labcorp's intrusion upon their seclusion, that include, among other things:

a. the loss in value of their individually-identifiable health information, or their property rights in this information, resulting

[60] *See* Poll: Huge Majorities Want Control Over Health Info, Healthcare Finance (Nov. 10, 2020), *https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info.*

from the unauthorized use of this information, including by Labcorp and Google;

b. the loss in value of the medical services they received, which included promises to maintain the confidentiality of their individually-identifiable health information and not to share or use this information for commercial purposes; and

c. the value Labcorp, Google, and others received from the commercial use of their individually-identifiable health information.

COUNT V
Unjust Enrichment

188. Plaintiffs incorporate the foregoing allegations as if fully set forth herein, except those that only/directly support their breach of contract claim.

189. Plaintiffs and the Class members have conferred direct and substantial benefits upon Labcorp by virtue of its unlawful transmission and use of their individually-identifiable health information for various commercial purposes.

190. These benefits include, but are not limited to:

a. Analyzing Plaintiffs' and the Class members' individually-identifiable health information to understand how people use its website and determine what ads people see on its website;

b. Profiting from selling access to Plaintiffs' and the Class members' individually-identifiable health information to Google;

c. Allowing Google to profit from access to Plaintiffs' and the Class members' individually-identifiable health information by building more fulsome profiles of their preferences and traits and selling more-targeted advertisements based on this information; and

d. Developing synergies between Labcorp and Google that incentivize each other to advertise, promote, and use the other's platforms and services to their mutual benefit.

191. Labcorp appreciated (*i.e.*, had knowledge of) the substantial benefits it received from Plaintiffs and the Class members because it: helped to design the computer code to collect

and transmit their individually-identifiable health information to Google; installed this computer code on the back-end of its website; and was actively involved in the knowing, surreptitious commercial use of this information.

192. Labcorp accepted and retained the benefits it derived from using Plaintiffs' and the Class members' individually-identifiable health information despite promising and agreeing, among other things, that: its website was a private and protected environment for communicating this information; it would keep this information private and protected; it would not disclose this information to third parties; and it would not use this information for commercial purposes without express notice and consent.

193. Under these circumstances, it is inequitable for Labcorp to retain the substantial benefits it received without paying value to Plaintiffs and the Class members measured by, among other things:

a. the value Labcorp received from Google and other sources for providing access to, and allowing use of, Plaintiffs' and the Class members' individually-identifiable health information;

b. the value Labcorp received from its own unauthorized commercial use of Plaintiffs' and the Class members' individually-identifiable health information, including from learning how people use its website, determining what ads people see on its website, and building more fulsome digital profiles of its patients' preferences and traits;

c. the loss in value of their individually-identifiable health information, or their property rights in this information, resulting from the unauthorized use of this information, including by Labcorp and Google; and

d. the loss in value of the medical services they received, which included promises to maintain the confidentiality of their individually-identifiable health information and not to share or use this information for commercial purposes.

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully ask this Court for an Order:

a. certifying this case as a class action, appointing Plaintiffs as Class Representatives, and appointing Stephan Zouras LLP as Class Counsel;

b. entering judgment for Plaintiffs and the Class members on their ECPA claim and awarding all damages available under 18 U.S.C. § 2520;

c. entering judgment for Plaintiffs and the Class members on their breach of contract claim and awarding all available damages;

d. entering judgment for Plaintiffs and the Class members on their negligence claim and requiring Labcorp to pay all available damages;

e. entering judgment for Plaintiffs and the Class members on their intrusion upon seclusion claim and requiring Labcorp to pay all available damages;

f. entering judgment for Plaintiffs and the Class members on their unjust enrichment claim and requiring Labcorp to pay all available damages;

g. awarding Plaintiffs and the Class members injunctive relief that includes an order barring Defendant from any further interception, transmission, or commercial use of Plaintiffs' and the Class members' communications with Labcorp's website absent express notice and informed consent so Plaintiffs and the Class members can, hereafter, communicate with Labcorp through its website to select, schedule, and receive important healthcare services without having these communications intercepted, disclosed to Google, and used for commercial purposes;

h. awarding pre- and post-judgment interest on all damages awarded;

i. awarding recovery of Plaintiffs' reasonable attorneys' fees and reimbursement of their litigation expenses; and

j. awarding any additional relief as hereafter identified, requested, or as needed to serve the interests of justice.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Respectfully Submitted,

Dated: February 13, 2024

/s/ *David J. Cohen*
David J. Cohen
STEPHAN ZOURAS, LLP
604 Spruce Street
Philadelphia, PA 19106
(215) 873-4836
dcohen@stephanzouras.com

Ryan F. Stephan
James B. Zouras
Teresa M. Becvar
Michael J. Casas
STEPHAN ZOURAS, LLP
222 W. Adams Street, Suite 2020
Chicago, Illinois 60606
(312) 233-1550
rstephan@stephanzouras.com
jzouras@stephanzouras.com
tbecvar@stephanzouras.com
mcasas@stephanzouras.com

Attorneys for Plaintiffs